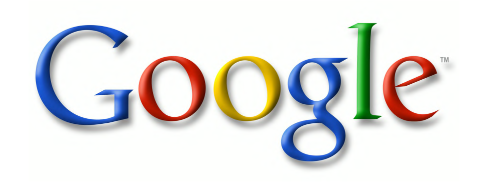
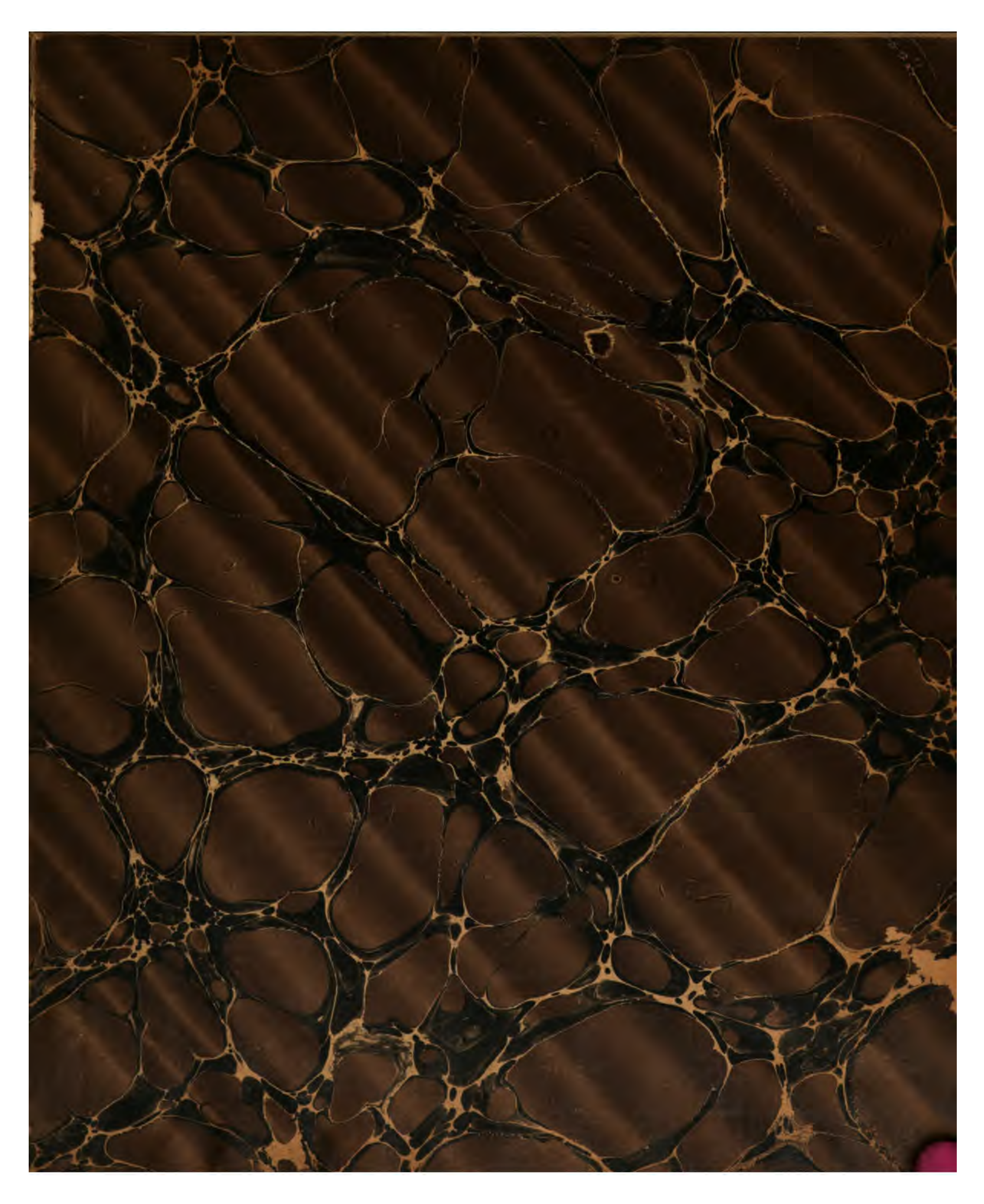




Math 2318.92.3
SIGILLUM ACADEMIAE HARVARDIANAE IN NOV ANG
CHRISTO ET ECCLESIAE
VE RI TAS
Harvard College Library
BOUGHT WITH INCOME
FROM THE BEQUEST OF
HENRY LILLIE PIERCE,
OF BOSTON.
Under a vote of the President and Fellows,
October 24, 1898.
10 April 1899
SCIENCE CENTER LIBRARY



N° D'ORDRE :
764.

THÈSES

PRÉSENTÉES

A LA FACULTÉ DES SCIENCES DE PARIS

POUR OBTENIR

LE GRADE DE DOCTEUR ÈS SCIENCES MATHÉMATIQUES,

Par M. MAILLET,

Ingénieur des Ponts et Chaussées à Montauban.

1re THÈSE. — Recherches sur les substitutions, et en particulier sur les groupes transitifs.

2e THÈSE. — Propositions données par la Faculté.

Soutenues le 7 Décembre 1892, devant la Commission d'examen.

MM. HERMITE, *Président.*
BOUSSINESQ, POINCARÉ, *Examinateurs.*

PARIS,

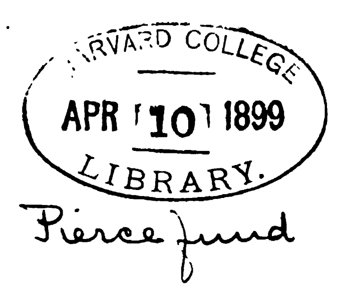
GAUTHIER-VILLARS ET FILS, IMPRIMEURS-LIBRAIRES

DU BUREAU DES LONGITUDES, DE L'ÉCOLE POLYTECHNIQUE,

Quai des Grands-Augustins, 55.

—

1892



ACADÉMIE DE PARIS.

FACULTÉ DES SCIENCES DE PARIS.

	MM.	
DOYEN	DARBOUX, professeur	Géométrie supérieure.
PROFESSEURS HONORAIRES	PASTEUR.	
	DUCHARTRE.	
PROFESSEURS	DE LACAZE-DUTHIERS	Zoologie, Anatomie, Physiologie comparée.
	HERMITE	Algèbre supérieure.
	TROOST	Chimie.
	FRIEDEL	Chimie organique.
	TISSERAND	Astronomie.
	LIPPMANN	Physique.
	HAUTEFEUILLE	Minéralogie.
	BOUTY	Physique.
	APPELL	Mécanique rationnelle.
	DUCLAUX	Chimie biologique.
	BOUSSINESQ	Mécanique physique et expérimentale.
	PICARD	Calcul différentiel et Calcul intégral.
	POINCARÉ	Calcul des probabilités, Physique mathématique.
	Yves DELAGE	Zoologie, Anatomie, Physiologie comparée.
	BONNIER	Botanique.
	DASTRE	Physiologie.
	DITTE	Chimie.
	MUNIER-CHALMAS	Géologie.
	GIARD	Zoologie. Évolution des êtres organisés.
PROFESSEURS ADJOINTS	WOLF	Physique céleste.
	CHATIN	Zoologie, Anatomie, Physiologie comparée.
	JOLY	Chimie.
SECRÉTAIRE	PHILIPPON.	

18531 PARIS. — IMPRIMERIE GAUTHIER-VILLARS ET FILS, QUAI DES GRANDS-AUGUSTINS, 55.

ERRATA.

—

Page 5, lignes 7 et 8, *au lieu de* le *Journal de Crelle*, *lisez* les *Mathematische Annalen*.

Page 6, ligne 21, *au lieu de* $p \geqq 5$, *lisez* primitifs, $p \geqq 11$.

Page 6, ligne 33, *après* premier), *ajoutez* s'ils sont primitifs.

Page 9, ligne 19, *au lieu de* le *Journal de Crelle, lisez* les *Mathematische Annalen*.

Page 10, lignes 1 et 2, *après* groupes, *ajoutez* transitifs.

Page 14, lignes 17 et 18, *supprimez* De plus, $\mathfrak{G}' = \frac{\mathfrak{G}}{\mathfrak{H}}$.

Page 27, ligne 4, *au lieu de* Γ, *lisez* G.

Page 55. ligne 1, *après* $N = p^m$, *ajoutez* et G primitif.

Page 55, ligne 3, *supprimer* s'il est primitif.

Page 55, ligne 10, *au lieu de* $4 + 2$, *lisez* $4h + 2$.

Page 55, ligne 22, *après* G, *ajoutez* primitif.

Page 74, ligne 2, *après* de G, *ajoutez* et qui eontient M.

Page 80, ligne 21, *au lieu de* $\frac{1}{2}\rho f(\rho f - 1)(\rho f - 2)$, *lisez* $\frac{1}{4}\rho f(\rho f - 1)(\rho f - 2)$.

Page 82, ligne 5, *au lieu de* on en a, *lisez* on peut en avoir.

Page 86, ligne 1, *au lieu de* 32, *lisez* 52.

Page 86, ligne 20, *au lieu de* $x_4;\ x_3 + h_4 x_4$, *lisez* $x_4;\ x_4 + h_4 x_3$.

Page 88, ligne 34, *au lieu de* $N \leqq 102$, *lisez* $N \leqq 62$.

Page 98, ligne 7, *au lieu de* $N \leqq 95$, *lisez* $N \leqq 102$.

Page 98, ligne 10, *après* groupe, *ajoutez* transitif.

Page 102, ligne 18, *après* groupes, *ajoutez* non symétriques ou alternés.

Page 102, ligne 25, *après* degrés.) *ajoutez* et un ou plusieurs groupes de classe 30.

Page 108, ligne 2, *après* à U, *ajoutez* contenant H.

Page 109, ligne 18, *au lieu de* par un, *lisez* par l'inverse d'un.

Page 114, ligne 10, *au lieu de* $\mathfrak{H}_q N_q$, *lisez* $q\mathfrak{H} N_q$.

Page 118, ligne 22, *au lieu de* h_q^p, *lisez* $h^{\frac{q}{p}}$.

18531 Paris. — Imprimerie Gauthier-Villars et fils, quai des Grands-Augustins, 55.

PREMIÈRE THÈSE.

RECHERCHES SUR LES SUBSTITUTIONS

ET EN PARTICULIER

SUR LES GROUPES TRANSITIFS.

HISTORIQUE DE LA THÉORIE DES SUBSTITUTIONS.

La théorie des substitutions entre un nombre n de lettres a pour but principal la formation de tous les groupes de substitutions qu'on peut former avec ces n lettres.

Jusqu'à présent l'histoire de cette théorie présente trois périodes principales.

Période de Galois et Cauchy. — Les fondateurs de la théorie, au moins sous la forme où on l'étudie actuellement, sont Galois et Cauchy.

Les travaux de Galois ont eu surtout pour but d'établir les fondements de la théorie des substitutions dans ses rapports avec celle des équations algébriques et de donner un procédé de construction des groupes dits *résolubles par radicaux*.

Quant à Cauchy, il a introduit une partie des termes actuellement en usage dans la théorie, donné la définition des groupes ou systèmes

de substitutions conjuguées, établi des théorèmes relatifs à la formation de ces groupes, et montré dans un cas particulier un théorème, complété plus tard par MM. Bertrand et Serret, au sujet des groupes de degré n et d'indice n ou $2n$. Cauchy a également donné ce théorème fondamental : *Si l'ordre d'un groupe est* $\equiv 0 \pmod p$, *p étant premier, ce groupe contient une substitution d'ordre p*; et la nomenclature des groupes primitifs pour les sept premiers degrés.

Période de M. Hermite. — Dans cette période nous citerons les noms de MM. Hermite, Serret, Kronecker et Mathieu.

M. Hermite introduit une notation nouvelle : il représente une substitution entre p^n lettres par une expression de la forme

$$|x; f(x)| \qquad (\text{mod}\, p)$$

dans laquelle, i étant une racine d'une congruence irréductible de degré $n \pmod p$, x prend les p^n valeurs

$$\alpha + \beta i + \ldots + \delta i^{n-1} \qquad (\text{mod}\, p),$$

ainsi que $f(x)$, $f(x)$ étant une fonction convenablement choisie. M. Hermite a établi à ce sujet un certain nombre de propriétés qui ont servi de base à M. Mathieu pour donner différentes catégories de groupes primitifs, établir dans un cas particulier un théorème généralisé ultérieurement par M. Sylow, donner la nomenclature des groupes primitifs pour les douze premiers degrés et montrer l'existence de groupes cinq fois transitifs des degrés 12 et 24.

Période de M. Jordan. — Cette période est la période actuelle. M. Jordan a étudié en particulier les groupes linéaires et ceux qu'ils contiennent (groupes abéliens, orthogonaux, etc.), construit les groupes résolubles par radicaux, donné, après M. Mathieu, de nombreuses limites de la transitivité des groupes qui ne contiennent pas le groupe alterné, introduit la notion des groupes simples et composés, de l'isomorphisme et de la classe. La classe d'un groupe est le nombre

de lettres déplacées par les substitutions du groupe qui en déplacent le moins (la substitution 1 étant exceptée). M. Jordan a montré que le nombre des groupes d'une classe donnée était limité, sauf pour les classes 2 et 3, ce qui établissait un nouveau mode de classification des groupes primitifs, déterminé les groupes primitifs dont la classe est un nombre premier, donné la nomenclature des groupes primitifs pour les dix-sept premiers degrés et les premières classes, et une foule d'autres propriétés.

Après M. Jordan, nous citerons MM. Sylow, Capelli, Netto et Walther Dyck.

Nous avons terminé l'historique en ce qui concerne la théorie pure des substitutions. Nous dirons cependant quelques mots des applications, bien qu'il n'en soit pas question dans notre thèse.

Nous citerons les applications à la symétrie des fonctions rationnelles et les applications géométriques faites par M. Jordan.

Nous citerons enfin les applications à la théorie des fonctions algébriques. Galois a établi le théorème fondamental et donné un criterium pour reconnaître et former les groupes résolubles par radicaux. M. Jordan a modifié ce criterium, ce qui lui a permis de construire ces groupes, étudié l'abaissement du degré des équations en partant de la notion des groupes simples et composés, et appliqué les résultats obtenus à un certain nombre d'équations célèbres. Il a étudié en particulier les équations modulaires et de la division des périodes dans les fonctions elliptiques et hyperelliptiques et en a déduit plusieurs théorèmes très importants, soit pour la théorie des substitutions, soit pour celle des équations.

M. Jordan a également montré que la solution d'une équation quelconque se ramenait toujours à celles d'équations dont les groupes sont primitifs, ce qui montre l'importance des groupes primitifs.

LISTE DES OUVRAGES CONSULTÉS.

Noms d'auteurs.	Ouvrages et Articles.
WALTHER DYCK.	*Gruppentheoretische Studien* (*Mathematische Annalen*, t. XX et XXII).
C. JORDAN.	*Traité des substitutions et des équations algébriques.*
	Théorèmes sur les groupes primitifs (*Journal de Liouville*, 1871; et *Comptes rendus*, 26 juin 1871).
	Sur la classification des groupes primitifs (*Comptes rendus*, 2 octobre 1871).
	Recherches sur les substitutions (*Journal de Liouville*, 1872; et *Comptes rendus*, 8 avril 1872).
	Énumération des groupes primitifs pour les dix-sept premiers degrés (*Comptes rendus*, 23 décembre 1872).
É. MATHIEU.	*Journal de Liouville*, 1861.
NETTO.	*Beweise und Lehrsaetze ueber transitive Gruppen* (*Journal de Crelle*, t. 83).
SERRET.	*Algèbre supérieure*, t. II.
SYLOW.	*Mathematische Annalen*, t. V.

INTRODUCTION.

Ce travail peut se diviser en trois Chapitres.

Chapitre I. — *Propriétés des groupes transitifs dont l'ordre égale le degré, et applications.*

Dans ce Chapitre nous complétons et généralisons des propriétés établies par MM. Jordan et Walther Dyck, l'un dans son *Traité des substitutions et des équations algébriques,* l'autre dans le *Journal de Crelle.*

Nous montrons, en particulier, qu'un groupe transitif quelconque peut toujours être dérivé d'un groupe transitif G dont l'ordre égale le degré, en n'y considérant que les substitutions opérées par ce groupe G entre les systèmes d'une répartition de ses lettres en systèmes de non-primitivité. Nous nous appuyons pour cela sur un théorème montrant qu'à tout groupe contenu dans G correspond une répartition des lettres de G en systèmes de non-primitivité et réciproquement, théorème qui est une généralisation d'un théorème de M. Jordan. Puis, d'un théorème de M. Walther Dyck, que nous établissons à nouveau, et d'après lequel, dans un groupe primitif, le groupe qui laisse une lettre immobile est maximum, et des propriétés précédentes nous concluons un procédé de recherche des groupes primitifs. Nous en faisons application, soit au groupe alterné de n lettres, soit au groupe des substitutions contenues dans le groupe linéaire (mod p) à deux indices et dont le déterminant est congru à un (mod p), p étant un nombre premier.

Nous montrons également, à l'aide des propriétés précédemment établies pour les groupes transitifs dont l'ordre égale le degré, que, d'un groupe simple quelconque G d'ordre $\mathcal{G}$ non premier, on peut toujours déduire un groupe primitif de degré $\mathcal{G}$, d'ordre $\mathcal{G}^2$, et dérivé du groupe transitif dont l'ordre égale le degré isomorphe à G et de son

conjoint. Aucun des groupes ainsi obtenus n'est de classe r^2, r étant un nombre premier. Nous faisons application de ce théorème :

1° Au groupe alterné de n lettres;

2° A un groupe simple contenu dans le groupe abélien à $2n$ indices $(\bmod p)$, p étant un nombre premier;

3° Aux groupes hypoabéliens;

4° Aux groupes de Steiner, qui ne donnent d'ailleurs que des groupes obtenus dans les cas précédents;

5° Au groupe linéaire à n indices $(\bmod 2)$.

Chapitre II. — *Des groupes transitifs de degré* N *et de classes* $N-1$, $N-2$ *ou* $N-3$.

Nous considérons successivement ces trois classes :

Classe $N-1$. — Nous montrons qu'un groupe transitif de classe $N-1$ et de degré N est toujours d'ordre $\mathfrak{N}(p\mathfrak{N}+1)$ avec $p\mathfrak{N}+1=N$, et que $N=p\mathfrak{N}+1$ est de la forme $(n\mathfrak{N}+1)(n'\mathfrak{N}+1)$ avec $n>0$, $n'>0$, si le groupe n'est pas primitif.

Nous distinguons ces groupes en deux catégories : la première, où les substitutions qui déplacent les N lettres forment avec l'unité un groupe transitif dont l'ordre égale le degré, c'est-à-dire N [1]; la deuxième, où ceci n'a pas lieu. Nous montrons que, pour les groupes de la deuxième catégorie, $p \geqq 5$. Nous examinons un certain nombre de valeurs particulières de N pour lesquelles nous montrons qu'un groupe transitif de classe $N-1$ et de degré N doit, soit ne pas être primitif, soit appartenir à la première catégorie, soit satisfaire à ces deux conditions réunies. Nous faisons voir qu'il n'y a aucun groupe primitif de classe $N-1=r^\alpha$ (r étant un nombre premier et α étant quelconque), qui ne soit linéaire, si $N \leqq 1000$.

Enfin nous concluons que les groupes primitifs de classe $N-1$ et de degré $N \leqq 101$ sont linéaires, avec $N=r^m$, les substitutions qui déplacent toutes les lettres pouvant être représentées par

$$|x_1, x_2, \ldots, x_m; x_1+\alpha_1, x_2+\alpha_2, \ldots, x_m+\alpha_m| \qquad (\bmod r),$$

les indices étant réels et α_i pouvant prendre une valeur quelconque

(1) Ces groupes sont tous linéaires et de degré r^m (r étant premier).

(mod r); en sorte que ces groupes appartiennent tous à la première catégorie.

Dans tous les cas particuliers examinés on ne peut avoir de groupe primitif de la deuxième catégorie.

Classe N — 2. — Nous montrons que les groupes transitifs de classe N — 2 et de degré N ont leur ordre égal à

$$\varkappa(p\varkappa + 1\,[(p\varkappa + 1)(q\varkappa + 1) + 1]$$

avec

$$N = (p\varkappa + 1)(q\varkappa + 1) + 1.$$

Nous vérifions ensuite que pour $N \leqq 102$ il n'y a d'autre groupe de classe N — 2 et de degré N primitif et une seule fois transitif qu'un groupe de degré 10, de classe 8 et d'ordre 60 cité par M. Jordan (*Comptes rendus*, 2 octobre 1871). De même, pour $N \leqq 102$, il ne peut exister de groupe de classe N — 2 et de degré N primitif et deux fois transitif, sauf si $N - 1 = r^\alpha$ (r étant un nombre premier, α étant quelconque).

Classe N — 3. — Nous montrons aussi bien pour cette classe que pour les deux précédentes que la classe d'un groupe primitif qu'elles renferment ne peut être égale à r^2 (r étant un nombre premier > 2).

Nous énonçons également, pour ceux de ces groupes qui appartiennent aux soixante-dix-sept ou aux cent premières classes suivant les cas et qui sont deux, trois ou quatre fois transitifs, un certain nombre de théorèmes, d'où l'on conclut des théorèmes correspondants pour les groupes de classe $N - i$ et de degré N $i - 1$, i ou $i + 1$ fois transitifs, i étant $\geqq 3$.

Enfin nous énonçons le théorème suivant, qui résulte directement des propriétés des groupes de classe N — 2 et de degré N transitifs :

Il n'existe aucun groupe de classe $4h + 1$ *et de degré* $4h + i + 1$ *qui soit au moins* $i - 1$ *fois transitif* ($i \geqq 2$).

Chapitre III. — *Sur une généralisation de la formule de Sylow.*

Nous étudions quelques propriétés respectives de deux groupes *échangeables* (Serret, *Algèbre supérieure*, t. II, p. 283) et nous

en concluons la formule de Sylow et une généralisation de cette formule. De la formule de Sylow nous tirons le théorème de Wilson et le théorème de Fermat; de la généralisation nous tirons cette propriété démontrée au Chapitre II : les groupes transitifs de classe $N - 1$ et de degré N ont leur ordre de la forme $\mathfrak{X}(p\mathfrak{X} + 1)$ avec $p\mathfrak{X} + 1 = N$.

Nous avons adopté les notations et les expressions employées par M. Jordan. Nous croyons devoir faire remarquer en particulier que M. Jordan représente le produit de S par T, c'est-à-dire la substitution qui équivaut à la substitution T opérée après la substitution S par ST, tandis que M. Serret le représente par TS. Il en résulte, par exemple, que le groupe H des substitutions

$$1, \quad 2, \quad \ldots, \quad h_{\mathfrak{H}}$$

est dit *permutable* à la substitution t si

$$t^{-1} h_i t = h_j,$$

quel que soit i dans la notation de M. Jordan, et si

$$t h_i t^{-1} = h_j,$$

quel que soit i dans la notation de M. Serret.

Nous disons indifféremment dans ce cas que t est permutable à H ou H permutable à t.

Enfin, en général, A, B, ..., G, H, ... étant des groupes de substitutions, nous désignons leurs ordres respectifs par $\mathfrak{A}$, $\mathfrak{B}$, ..., $\mathfrak{G}$, $\mathfrak{H}$, ...

CHAPITRE I.

PROPRIÉTÉS DES GROUPES TRANSITIFS DONT L'ORDRE ÉGALE LE DEGRÉ, ET APPLICATIONS.

M. Jordan a montré qu'un groupe quelconque de substitutions avait toujours un isomorphe holoédrique transitif et dont l'ordre égale le degré. Il a montré également pour les groupes transitifs dont l'ordre égale le degré les propriétés suivantes :

1° Les substitutions de ces groupes, à part la substitution 1, sont régulières et déplacent toutes les lettres.

2° Un cycle quelconque d'une substitution d'un de ces groupes contenant p lettres donne un système d'une répartition des lettres du groupe en systèmes de non-primitivité de p lettres, p étant un nombre quelconque (ou plus simplement un système d'une répartition des lettres du groupe p à p).

3° Les groupes transitifs dont l'ordre égale le degré sont conjoints deux à deux de telle sorte que chacun d'eux soit formé par l'ensemble des substitutions échangeables à celles de son conjoint (*Traité des substitutions et des équations algébriques*, p. 58 à 60).

D'autre part, M. Walther Dyck, dans le *Journal de Crelle*, a généralisé la deuxième de ces propositions et montré de plus le théorème suivant :

La condition nécessaire et suffisante pour qu'un groupe transitif quelconque G *soit primitif est que le groupe formé par l'ensemble des substitutions de* G *qui laissent une lettre donnée immobile soit maximum dans* G, *c'est-à-dire tel que, en le combinant avec une substitution quelconque de* G, *on obtienne le groupe* G.

Nous allons nous proposer de compléter et de généraliser les propriétés précédentes, ou d'en simplifier les démonstrations, puis d'en faire quelques applications.

Théorèmes relatifs aux groupes dont l'ordre égale le degré.

Théorème I. — *A tout groupe* H *contenu dans un groupe* G *dont l'ordre égale le degré* $\mathfrak{g}$ *correspond une répartition des lettres de* G *en systèmes de non-primitivité de* $\mathfrak{h}$ *lettres,* $\mathfrak{h}$ *étant l'ordre de* H; *et réciproquement.*

En effet, soient a', a'', ... les lettres que H substitue à a' : ces lettres doivent être en nombre égal à $\mathfrak{h}$, sans quoi une des substitutions de H autre que l'unité laisserait une lettre immobile. De plus H permute évidemment ces lettres exclusivement entre elles. Enfin, toute substitution de G qui substitue une de ces lettres à une autre de ces lettres fait partie de H.

Soit b' une autre lettre,

$$g = (a', b', \ldots)\ldots$$

une substitution de G non contenue dans H; g remplacera les $\mathfrak{h}$ lettres a', a'', ... par $\mathfrak{h}$ autres lettres b', b'', ..., et aucune des lettres b', b'', ... ne sera identique à une des lettres a', a'', ... sans quoi b' serait identique à une de ces lettres, contrairement à l'hypothèse.

Si alors

$$1, \quad h_2, \quad \ldots, \quad h_{\mathfrak{h}}$$

sont les substitutions de H, les substitutions

$$(1) \qquad g, \quad h_2 g, \quad \ldots, \quad h_{\mathfrak{h}} g$$

en nombre $\mathfrak{h}$ remplacent les lettres a exclusivement par des lettres b et sont différentes. Une substitution quelconque S de G de la forme

$$S = (a^{(i)} b^{(j)} \ldots)\ldots$$

est renfermée dans la suite (1), car cette suite renferme toujours une substitution de la forme $(a^{(i)} b^{(j)} \ldots)\ldots$, et G ne renferme qu'une substitution de cette forme, puisque toutes les substitutions déplacent toutes les lettres.

Considérant alors une lettre quelconque c' non comprise parmi les lettres a ou b et la substitution $(a'c'\ldots)\ldots = g'$ contenue dans G, on voit encore que les substitutions

$$(2) \qquad g', \quad h_2 g', \quad \ldots, \quad h_{\mathfrak{H}} g'$$

remplacent les lettres a par $\mathfrak{H}$ autres lettres c', c'', ... dont aucune ne coïncide avec une des lettres a ou b.

En continuant de la sorte, on forme $\frac{\mathfrak{G}}{\mathfrak{H}}$ lignes,

$$(3) \qquad \begin{cases} 1, & h_2, & \ldots, & h_{\mathfrak{H}}, \\ g, & h_2 g, & \ldots, & h_{\mathfrak{H}} g, \\ g', & h_2 g', & \ldots, & h_{\mathfrak{H}} g', \\ \ldots & \ldots & \ldots & \ldots, \end{cases}$$

contenant toutes les substitutions de G et $\frac{\mathfrak{G}}{\mathfrak{H}}$ systèmes de $\mathfrak{H}$ lettres, telles que deux systèmes n'aient aucune lettre commune et que ces systèmes renferment les $\mathfrak{G}$ lettres de G,

$$(4) \qquad \begin{cases} a', & a'', & \ldots, & a^{(\mathfrak{H})}, \\ b', & b'', & \ldots, & b^{(\mathfrak{H})}, \\ c', & c'', & \ldots, & c^{(\mathfrak{H})}, \\ \ldots & \ldots & \ldots & \ldots \end{cases}$$

De plus, les substitutions de la $j^{\text{ième}}$ ligne du tableau (3) remplacent a', a'', ..., $a^{(\mathfrak{H})}$ exclusivement par les lettres de la $j^{\text{ième}}$ ligne du tableau (4).

Je dis que le tableau (4) donne une répartition des lettres de G en systèmes de non-primitivité de $\mathfrak{G}$ lettres.

En effet, une substitution A de G qui remplace $b^{(\alpha)}$ par $c^{(\beta)}$ est toujours le produit d'une substitution

$$B = (b^{(\alpha)} a' \ldots)\ldots,$$

qui est l'inverse d'une substitution de la deuxième ligne du tableau (3)

par la substitution

$$C = (a' c^{(\beta)} \ldots) \ldots,$$

qui est une substitution de la troisième ligne de ce tableau. Or B remplace les lettres b par des lettres a; C remplace les lettres a exclusivement par des lettres c. Donc $A = BC$ remplace les lettres b exclusivement par des lettres c. Par suite, une substitution quelconque de G remplace toujours les lettres d'une des lignes du tableau (4) par les lettres d'une ligne du même tableau. C. Q. F. D.

La réciproque est évidente : car si le tableau (4) représente une répartition des lettres en systèmes de $\mathfrak{H}$ lettres admise par G, les substitutions de la forme $(a' a^{(i)} \ldots) \ldots$, qui sont évidemment en nombre $\mathfrak{H}$, permutent exclusivement entre elles les $\mathfrak{H}$ lettres de la première ligne du tableau (4); comme elles jouissent seules de cette propriété, elles forment un groupe H. C. Q. F. D.

Isomorphisme du groupe G avec les groupes formés par les déplacements entre les systèmes de non-primitivité admis par G.

Conservant les notations précédentes, nous considérerons la répartition (4) et désignerons par $\alpha, \beta, \gamma, \ldots$ chacune des lignes de (4) ou chacun des systèmes en nombre $\frac{\mathcal{G}}{\mathfrak{H}}$ de cette répartition.

Théorème II. — *Si* H *est un groupe contenu dans un groupe* G *transitif dont l'ordre égale le degré, si* $\alpha, \beta, \gamma, \ldots$ *désignent les systèmes d'une répartition des lettres de* G *correspondant à* H *et si* M *est le groupe le plus général de* H *permutable aux substitutions de* G, *le groupe isomorphe à* G *formé par les substitutions opérées par* G *entre* $\alpha, \beta, \gamma, \ldots$ *est d'ordre* $\frac{\mathcal{G}}{\mathfrak{M}}$ *et transitif entre* $\frac{\mathcal{G}}{\mathfrak{H}}$ *lettres.* M *est formé par l'ensemble des substitutions de* G *qui permutent exclusivement entre elles les lettres de chaque système.*

En effet, soit G′ ce groupe isomorphe à G : son degré est évidemment $\frac{\mathcal{G}}{\mathfrak{H}}$. D'ailleurs, deux substitutions de G ne peuvent donner entre les $\alpha, \beta, \gamma, \ldots$ deux substitutions identiques, qui se réduiraient alors à

une seule, que si elles appartiennent à une même ligne du tableau (3), car dans ce tableau les substitutions de la première ligne laissent toutes α immobile; celles de la deuxième remplacent α par β, etc. Si $h_i g$ et $h_j g$, par exemple, sont ces deux substitutions, h_i et h_j donnent entre les $\alpha, \beta, \gamma, \ldots$ deux substitutions identiques, et réciproquement. Le nombre des substitutions $h_i, h_j, \ldots$ qui deviennent ainsi identiques est égal au nombre des substitutions de H qui deviennent égales à 1. Ces substitutions forment un groupe M d'ordre $\mathfrak{M}$ dont les substitutions sont de la forme $\begin{pmatrix} \alpha\beta\gamma\ldots \\ \alpha\beta\gamma\ldots \end{pmatrix}$, et réciproquement toutes les substitutions de cette forme deviennent égales à 1 et font partie de M. Chaque ligne du tableau (3) donnera alors dans G′ $\frac{\mathfrak{H}}{\mathfrak{M}}$ substitutions différentes et différentes de celles données par les autres lignes; G′ sera donc d'ordre $\frac{\mathfrak{G}}{\mathfrak{H}} \frac{\mathfrak{H}}{\mathfrak{M}} = \frac{\mathfrak{G}}{\mathfrak{M}}$.

Le groupe M est tel que les substitutions de G le transforment en lui-même. C'est le plus général des groupes de H jouissant de cette propriété, sans quoi, M′ étant ce groupe, et toutes ses substitutions, étant de la forme $\begin{pmatrix} \alpha\ldots \\ \alpha\ldots \end{pmatrix}$, sont de la forme $\begin{pmatrix} \beta\ldots \\ \beta\ldots \end{pmatrix}$, de la forme $\begin{pmatrix} \gamma\ldots \\ \gamma\ldots \end{pmatrix}$, etc., par suite de la forme $\begin{pmatrix} \alpha\beta\gamma\ldots \\ \alpha\beta\gamma\ldots \end{pmatrix}$ et font partie de M.

Théorème III. — *Si* H′ *est un groupe contenant* H *et contenu dans* G, H′ *permute exclusivement entre elles* $\frac{\mathfrak{H}'}{\mathfrak{H}}$ *des lettres* $\alpha, \beta, \gamma, \ldots$, *et le groupe des substitutions opérées par* G *entre les lettres* $\alpha, \beta, \gamma, \ldots$ *admet une répartition de ces lettres* $\frac{\mathfrak{H}'}{\mathfrak{H}}$ *à* $\frac{\mathfrak{H}'}{\mathfrak{H}}$, *correspondant à* H′, *qui laisse immobile un des systèmes de cette répartition. La réciproque est vraie.*

En effet, H′ contient toutes les substitutions de la forme $\begin{pmatrix} \alpha\ldots \\ \alpha\ldots \end{pmatrix}$; si H′ contient une substitution de la forme $(\alpha\beta\ldots)\ldots$, il les contiendra toutes, etc. : ce qui montre que H′ permute exclusivement entre elles $\frac{\mathfrak{H}'}{\mathfrak{H}}$ des lettres $\alpha, \beta, \gamma, \ldots$. On voit, d'ailleurs, comme au théorème I, qu'une substitution quelconque de G remplace ces $\frac{\mathfrak{H}'}{\mathfrak{H}}$ lettres par $\frac{\mathfrak{H}'}{\mathfrak{H}}$ dif-

férentes, et l'on répartit de même les $\frac{\mathfrak{G}}{\mathfrak{H}}$ lettres $\alpha, \beta, \gamma, \ldots$ en $\frac{\mathfrak{G}}{\mathfrak{H}'}$ lignes de $\frac{\mathfrak{H}'}{\mathfrak{H}}$ lettres, formant un tableau analogue au tableau (4), et dont chacune forme un système d'une répartition des $\frac{\mathfrak{G}}{\mathfrak{H}}$ lettres $\alpha, \beta, \ldots, \frac{\mathfrak{H}'}{\mathfrak{H}}$ à $\frac{\mathfrak{H}'}{\mathfrak{H}}$.

La réciproque s'obtient en remarquant que, si H′ est le groupe de G laissant immobile un des systèmes de la répartition de ces lettres α, $\beta, \gamma, \ldots, \frac{\mathfrak{H}'}{\mathfrak{H}}$ à $\frac{\mathfrak{H}'}{\mathfrak{H}}$, H′ contient H laissant α immobile, et que H est d'ordre $\mathfrak{H}' : \left(\frac{\mathfrak{H}'}{\mathfrak{H}}\right) = \mathfrak{H}$. C. Q. F. D.

Corollaire. — La condition nécessaire et suffisante pour que H soit contenu dans un groupe H′ d'ordre $\mathfrak{H}' = n\mathfrak{H}$ dont les substitutions sont permutables à H, H′ étant le groupe le plus général jouissant de cette propriété, est que H laisse immobile n des lettres $\alpha, \beta, \gamma, \ldots$, et pas d'autres.

Théorème IV. — *Si* H *est un groupe maximum dans* G, *le groupe* G′, *isomorphe à* G, *formé par les substitutions opérées par* G *entre les systèmes* $\alpha, \beta, \gamma, \ldots$, *est primitif et d'ordre* $\frac{\mathfrak{G}}{\mathfrak{M}}$, M *étant le groupe le plus général de* H *permutable aux substitutions de* G. *De plus,* $\mathfrak{G}' = \frac{\mathfrak{G}}{\mathfrak{H}}$.

Si $\mathfrak{M} = \mathfrak{H}$, $\frac{\mathfrak{G}}{\mathfrak{M}}$ *est premier. Sinon, le groupe* H′, *isomorphe de* H *et contenu dans* G′, *d'ordre* $\mathfrak{H}' = \frac{\mathfrak{H}}{\mathfrak{M}}$, *ne laisse immobile qu'une des lettres* $\alpha, \beta, \gamma, \ldots$. *Si* $\mathfrak{M} = 1$ *ou si l'isomorphisme est holoédrique,* G′ *est simple ou contient un groupe* N′ *plus petit, transitif entre les lettres* $\alpha, \beta, \gamma, \ldots$ *et permutable aux substitutions de* G′.

Réciproquement, H *étant donné, si* G′ *est primitif,* H *est maximum dans* G.

La plupart de ces propriétés résultent directement des théorèmes précédents. Dans le cas où $\mathfrak{M} = 1$, c'est-à-dire où l'isomorphisme de G et G′ est holoédrique, si G n'est pas simple, soit N le plus petit groupe

de G permutable aux substitutions de G, par suite aux substitutions de H. Il n'est pas contenu dans H et le groupe dérivé de N et de H est G. Si Ω est l'ordre du groupe commun à N et à H, $\mathcal{G} = \frac{\mathfrak{H}\mathfrak{N}}{\Omega}$. Le nombre des substitutions de N′ qui laissent une des lettres $\alpha, \beta, \gamma, \ldots$, donnée, immobile, N′ étant l'isomorphe de N contenu dans G′, est Ω. On voit donc que N′ est transitif entre $\frac{\mathcal{G}}{\mathfrak{H}}$ lettres, par suite transitif entre les lettres $\alpha, \beta, \gamma, \ldots$. Cette propriété résulte d'ailleurs d'un théorème de M. Jordan disant que, si un groupe B est contenu dans un groupe A primitif et est permutable à ses substitutions, il est forcément transitif (¹). (*Traité des substitutions*, p. 41.)

Le groupe H′ isomorphe à H, G′ et G, étant holoédriquement ou non isomorphes, ne laisse immobile qu'une des $\frac{\mathcal{G}}{\mathfrak{H}}$ lettres $\alpha, \beta, \gamma, \ldots$. Par transformation, on obtient $\frac{\mathcal{G}}{\mathfrak{H}}$ groupes isomorphes à H′ holoédriquement et laissant chacun respectivement une des lettres $\alpha, \beta, \gamma, \ldots$ immobiles.

Théorème V. — *Étant donnés un groupe transitif* G *contenant un groupe* H *formé des substitutions de* G *qui laissent une lettre a immobile*,

$$(5) \qquad 1,\ h_2,\ h_3,\ \ldots,\ h_{\mathfrak{H}},$$

les substitutions de H,

$$(6) \qquad \left\{\begin{array}{lllll} 1, & h_2, & h_3, & \ldots, & h_{\mathfrak{H}}, \\ g_2, & h_2 g_2, & h_3 g_2, & \ldots, & h_{\mathfrak{H}} g_2, \\ \ldots, & \ldots\ldots, & \ldots\ldots, & \ldots, & \ldots\ldots, \\ g_{\frac{\mathcal{G}}{\mathfrak{H}}}, & h_2 g_{\frac{\mathcal{G}}{\mathfrak{H}}}, & h_3 g_{\frac{\mathcal{G}}{\mathfrak{H}}}, & \ldots, & h_{\mathfrak{H}} g_{\frac{\mathcal{G}}{\mathfrak{H}}} \end{array}\right.$$

les substitutions de G, *on en déduit un groupe* G′ *transitif dont*

(¹) Si N′ a μ facteurs de composition, ces facteurs sont tous égaux à l'un d'entre eux t et l'ordre $\mathfrak{N}$ de N′ est égal à t^μ (Jordan, *Traité des substitutions*, p. 48 à 50).

l'ordre égale le degré $\mathcal{G}$ en considérant les substitutions opérées par chaque substitution de G *entre les symboles* (6), *et* G′ *est holoédriquement isomorphe à* G. *Réciproquement, en considérant le groupe isomorphe à* G′ *formé par les substitutions opérées par* G′ *entre les systèmes d'une répartition des lettres de* G′ *correspondant à* H′, *isomorphe de* H *dans* G′, *on obtient de nouveau le groupe* G *à la notation près.*

La première partie du théorème se démontre par le procédé connu : la substitution T′ de G′ correspondant à la substitution T de G sera, en désignant les substitutions de G par

$$1, \quad T_2, \quad \ldots, \quad T_{\mathcal{G}}$$

et les substitutions

$$T, \quad T_2T, \quad \ldots, \quad T_{\mathcal{G}}T,$$

qui sont les mêmes à l'ordre près, par

$$S_1, \quad S_2, \quad \ldots, \quad S_{\mathcal{G}},$$

$$T' = \begin{pmatrix} 1 & T_2 & \ldots & T_{\mathcal{G}} \\ S_1 & S_2 & \ldots & S_{\mathcal{G}} \end{pmatrix},$$

à condition de remplacer les symboles S par les symboles T qui désignent respectivement les mêmes substitutions.

Pour démontrer la réciproque, nous remarquerons que T′ remplace les symboles d'une des lignes du tableau (6) par les symboles d'une autre de ces lignes, c'est-à-dire que chacune de ces lignes forme un système d'une répartition des lettres déplacées par G′, $\mathfrak{H}$ à $\mathfrak{H}$. Désignons ces lignes respectivement par α, β, γ, ... Si T fait partie de H, T′ permute évidemment exclusivement entre elles les lettres de la première ligne du tableau (6), et H′ permute exclusivement entre elles les lettres de α.

Si $g_2 = (ab\ldots)\ldots$, b étant une autre lettre de G, les substitutions de G qui sont de la forme $(ab\ldots)\ldots$ sont celles de la deuxième ligne du tableau (6), et les substitutions correspondantes dans G′ sont de la forme $(\alpha\beta\ldots)\ldots$.

De même, pour $g_3 = (ac\ldots)\ldots$, etc.

Nous faisons ainsi correspondre les lettres a, b, c, ... aux lettres α, β, γ, ... Pour montrer la deuxième partie de notre théorème, il suffit de faire voir qu'à une substitution

$$A = (bc\ldots)\ldots$$

de G correspond dans G′ une substitution de la forme

$$(\beta\gamma\ldots)\ldots,$$

ou une substitution qui remplace la deuxième ligne de (6) par la troisième.

Or les substitutions de cette deuxième ligne sont de la forme

$$B = h_i g_2 = (ab\ldots)\ldots.$$

Celles de la troisième sont de la forme

$$C = h_j g_2 = (ac\ldots)\ldots,$$

et

$$A = B^{-1}C = g_2^{-1} h_i^{-1} h_j g_2.$$

A A correspond dans G′ une substitution qui remplace

$$g_2, \quad h_2 g_2; \quad \ldots, \quad h_{\mathfrak{g}} g_2$$

par

$$h_i^{-1} h_j g_3, \quad h_2 h_i^{-1} h_j g_3, \quad \ldots, \quad h_{\mathfrak{g}} h_i^{-1} h_j g_3,$$

c'est-à-dire β par γ.

Les lettres a, b, c, ... de G correspondront alors avec les systèmes α, β, γ, ... de G′ de telle sorte qu'à une substitution

$$(ef\ldots)\ldots \text{ de G}$$

correspondra une substitution

$$(\varepsilon\varphi\ldots)\ldots \text{ de G}',$$

ε correspondant à e et φ à f.

Le groupe isomorphe à G′, formé par les substitutions opérées par G′ entre les systèmes α, β, γ, ... sera donc précisément le

groupe G où l'on aura remplacé a, b, c, ... respectivement par α, β, γ, ...

On voit ainsi que tous les isomorphes holoédriques de G, conduisant au même groupe d'ordre égal au degré et transitif, se déduisent du groupe G' par le procédé qu'on vient d'indiquer.

De ce théorème, joint aux théorèmes précédents, on conclut quelques autres théorèmes :

Théorème VI. — *La condition nécessaire et suffisante pour qu'un groupe transitif quelconque soit primitif est que le groupe formé par les substitutions qui laissent une lettre donnée immobile soit maximum* (théorème de M. Walther Dyck).

En effet, soient respectivement G et H ces deux groupes, G' l'isomorphe de G transitif et dont l'ordre égale le degré $\mathfrak{z}'$, H' le groupe de G' isomorphe de H. D'après le théorème V, G se déduit de G' en considérant les substitutions opérées par G' entre les systèmes de la répartition admise par G' et correspondante à H', et H est le groupe formé par celles de ces substitutions qui font partie de H'. D'après le théorème IV, la condition nécessaire et suffisante pour que G soit primitif est que H y soit maximum. C. Q. F. D.

Théorème VII. — *Étant donné un groupe transitif* G *où le groupe* H, *formé par les substitutions de* G *qui laissent une lettre donnée immobile, est contenu dans un groupe* H' *plus grand que* H *et plus petit que* G, G *admet une répartition de ses lettres en systèmes de non-primitivité de* $\frac{\mathfrak{z}'}{\mathfrak{z}}$ *lettres et réciproquement.*

Comme dans le théorème précédent, il suffit de considérer le groupe G' qui est l'isomorphe de G transitif et dont l'ordre égale le degré, puis d'en déduire à nouveau le groupe G et les groupes H' et H qu'il contient, en appliquant le théorème III. C. Q. F. D.

Théorème VIII. — *Étant donné un groupe* G *transitif,* H *le groupe des substitutions de* G *qui laissent une lettre donnée immobile, la condition nécessaire et suffisante pour que* H *soit contenu dans un groupe* H' *de* G *d'ordre* $\mathfrak{z}' = n\mathfrak{z}$, *dont les substitutions*

sont permutables à H, H′ *étant le groupe le plus général jouissant de cette propriété, est que* H *laisse immobile n des lettres de* G *et pas d'autres. Dans ce cas, le degré* N *est* $\equiv 0 \pmod{n}$.

THÉORÈME VIII *bis*. — *Étant donné un groupe* G *transitif, mais non primitif, la condition nécessaire et suffisante, pour que les substitutions opérées par* G *entre les systèmes d'une répartition forment un groupe primitif* G′, *est que cette répartition soit maxima, ou que le groupe des substitutions qui permutent exclusivement entre elles les lettres d'un des systèmes de cette répartition soit maximum.*

Application des propriétés précédentes à la recherche des groupes primitifs.

Étant donné un groupe quelconque G et le groupe isomorphe transitif dont l'ordre égale le degré $\mathcal{G}$, on en déduira à l'aide des théorèmes précédents un certain nombre de groupes isomorphes à G. L'application du théorème IV donnera, en particulier, ceux qui sont primitifs. Si H est un groupe maximum dans G, on lui fait correspondre d'après ce théorème un groupe primitif G′ isomorphe à G. D'ailleurs S étant une substitution qui n'est comprise ni dans H, ni dans un de ses transformés par les substitutions de G, on en déduira, dans bien des cas, un groupe K maximum dans G et qui ne sera pas isomorphe de H et un groupe primitif correspondant différent de G′.

Ceci a lieu, en particulier, pour les groupes simples de degré quelconque. Donc :

THÉORÈME IX. — *D'un groupe simple quelconque, primitif, de degré quelconque, on déduira toujours, à l'aide du théorème IV, au moins deux groupes primitifs différents, dont l'un coïncidera, d'ailleurs, avec le groupe donné, qui est primitif.*

Nous ne considérons pas, bien entendu, comme différents, deux groupes qui ne diffèrent que par la façon de désigner les lettres qu'ils déplacent.

Nous allons appliquer ce qui précède à deux catégories de groupes.

I. — Groupe alterné G de n éléments ($n > 4$).

Nous savons que ce groupe est simple. Soit G′ isomorphe dont l'ordre égale le degré et qui est transitif; un groupe quelconque H de G donne alors, par l'application des théorèmes II et IV à G′ et à H′ isomorphe de H dans G′, un groupe transitif de degré $\frac{\mathfrak{G}}{\mathfrak{H}}$ et d'ordre $\mathfrak{G}$.

Si H est un groupe alterné de m des éléments de G, $\mathfrak{H} = \frac{m!}{2}$, $\mathfrak{G} = \frac{n!}{2}$ et le groupe obtenu est transitif entre $\frac{n!}{m!}$ lettres. Si $m = n - 1$, H est maximum dans G et l'on obtient à nouveau le groupe alterné de n éléments.

En général, si l'on remarque que $\frac{\mathfrak{G}}{\mathfrak{H}} = \frac{i}{2}$, i étant l'indice du groupe H (Serret, *Algèbre supérieure*, t. II, p. 314), on voit que le groupe transitif obtenu de degré $\frac{i}{2}$ sera primitif, si aucun des diviseurs de $\frac{i}{2}$ différents de $\frac{i}{2}$ n'est $\geqq n$, car si ce groupe n'était pas primitif, on en conclurait un groupe primitif de degré $< n$ et d'ordre $\mathfrak{G} = \frac{n!}{2}$, ce qui est évidemment absurde. Donc :

Théorème X. — *A tout groupe* H *contenu dans le groupe alterné* G *de n éléments et d'indice $i = \frac{2\mathfrak{G}}{\mathfrak{H}}$, correspondra un groupe primitif isomorphe à* G, *si $\frac{i}{2}$ n'admet aucun diviseur différent de $\frac{i}{2}$ et $\geqq n$.*

Si l'on suppose que n soit diviseur de $\mathfrak{H}$, on voit de même le théorème suivant :

Théorème XI. — *A tout groupe* H *maximum et d'ordre divisible par n, contenu dans le groupe alterné* G *de n éléments (n étant quelconque), correspondra un groupe primitif d'ordre $\mathfrak{G}$ isomorphe à* G *et de degré $\geqq n + 1$, si n est premier et $\geqq n$, si n est quelconque.*

Si ce degré est égal à $n + 1$, le groupe primitif obtenu est au moins 2 fois transitif, quand n est premier.

Comme application du premier de ces théorèmes, nous considérerons le cas où n égale 5.

Si $n = 5$, le groupe alterné de 5 éléments contient un groupe maximum de degré 5 et d'ordre 10 pour lequel $\frac{i}{2} = 6$. Le théorème X donne un groupe primitif de degré 6, d'ordre 6.5.2, deux fois transitif, de classe 4.

Si $n = 7$, le groupe alterné de 7 éléments contient un groupe de degré 7 et d'ordre 168 (SERRET, *Algèbre supérieure*, t. II, p. 412), pour lequel $\frac{i}{2} = 15$. On en déduit, par le théorème XI, un groupe primitif de degré 15 et d'ordre 15.168.

Si $n = 8$, le groupe alterné de 8 éléments contient un groupe de degré 8 et d'ordre 8.7.6.4 (JORDAN, *Comptes rendus*, 2 octobre 1871). On en déduit, par le théorème XI, un groupe primitif K de degré $\frac{i}{2} = 15$ et d'ordre 15.8.7.6.4.

L'application du théorème XI au cas de $n = 5$ donne le résultat déjà obtenu par le théorème X.

Remarque. — Nous avons vu que d'un groupe quelconque H, contenu dans le groupe alterné G, on tire un groupe d'ordre $\mathcal{G}$, de degré $\frac{\mathcal{G}}{\mathfrak{H}} = \frac{i}{2}$ transitif.

Si l'on avait $\frac{i}{2} < n$, le groupe obtenu de degré $< n$ serait d'ordre $\mathcal{G} = \frac{n!}{2}$, ce qui est absurde. Donc :

L'indice d'un groupe H *contenu dans le groupe alterné* G *de* n *éléments,* H *ne contenant pas toutes les substitutions de* G, *est* $\geqq 2n$.

On en conclut facilement le théorème de M. Bertrand :

THÉORÈME. — *L'indice d'un système de substitutions conjuguées formées avec n lettres ne peut être en même temps supérieur à* 2 *et inférieur à n.* (SERRET, *Algèbre supérieure*, t. II, p. 319).

On peut encore, comme application du théorème VI, déduire du

groupe symétrique ou du groupe alterné de n éléments une catégorie de groupe primitif.

M. Jordan cite, dans son *Énumération des groupes primitifs pour les* 17 *premiers degrés :*

Les groupes de degré $\frac{n(n-1)}{2}$ *formés par les déplacements que les groupes symétriques ou alternés entre les n lettres* $a_1, a_2, \ldots, a_n$ *font éprouver aux* $\frac{n(n-1)}{2}$ *produits binaires* $a_1a_2, a_1a_3, \ldots, a_1a_n, a_2a_3, \ldots$, *n étant* > 4.

D'une façon générale, on peut dire :

THÉORÈME. — *Les groupes de degré* $C_n^\alpha = \frac{n(n-1)\ldots(n-\alpha+1)}{1.2\ldots\alpha}$ *formés par les déplacements que les groupes symétriques ou alternés entre n lettres* $a_1, a_2, \ldots, a_n$ *font éprouver aux* C_n^α *produits de ces lettres* α *à* α *sont primitifs si* $n > 4$ *et* $\alpha \neq \frac{n}{2}$.

Car les groupes obtenus sont évidemment transitifs, et l'on voit facilement que les substitutions des groupes symétrique ou alterné qui laissent un de ces produits arbitrairement choisi immobile forment un groupe maximum.

Les groupes de degré C_n^α et $C_n^{n-\alpha}$ sont d'ailleurs identiques à la notation près, parce que, à un produit de α lettres, on peut faire correspondre celui des $n-\alpha$ autres.

Enfin, dans le cas de $n = 2\alpha$, on obtient, à l'aide des théorèmes I à VIII *bis,* des groupes primitifs isomorphes aux groupes symétrique ou alterné et de degré $\frac{1}{2} C_n^{\frac{n}{2}}$. Dans ce cas, n est d'ailleurs pair.

II. — GROUPES CONTENUS DANS LE GROUPE LINÉAIRE (MOD p) A 2 INDICES ET DONT LES SUBSTITUTIONS ONT LEUR DÉTERMINANT CONGRU A 1 (MOD p) (p ÉTANT PREMIER).

Nous verrons plus loin que ces groupes sont isomorphes à des groupes d'ordre égal au degré transitif, ce degré étant $p\frac{p^2-1}{2}$, et

que ces derniers groupes renferment des groupes d'ordre $p\frac{p-1}{2}$. Comme ils sont simples, on en conclut des groupes de degré $p+1$, deux fois transitifs, d'ordre $(p+1)p\frac{p-1}{2}$, et de classe $p-1$, obtenus, d'ailleurs, par MM. Mathieu et Jordan.

Des groupes maxima contenus dans un groupe transitif dont l'ordre égale le degré et non permutable à ses substitutions, et des répartitions correspondantes.

Soit G le groupe transitif dont l'ordre égale le degré, H_α un groupe maximum contenu dans G,

$$(7)\qquad \begin{cases} a', & a'', & \ldots, & a^{(\mathfrak{H})} & \text{ou} & \alpha, \\ b', & b'', & \ldots, & b^{(\mathfrak{H})} & \text{ou} & \beta, \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots, \end{cases}$$

les systèmes d'une répartition des lettres de G, $\mathfrak{H}$ à $\mathfrak{H}$, correspondante à H_α, α étant l'unique système de cette répartition dont H_α permute exclusivement entre elles toutes les lettres. En transformant H_α par les substitutions de G, on obtient $\frac{\mathcal{G}}{\mathfrak{H}}$ groupes H_α, H_β, ... dont chacun permute exclusivement entre elles les lettres d'un des systèmes α, β, ...

Soit a'_1 une lettre non comprise dans α, $a'_1, a''_1, \ldots, a_1^{(\mathfrak{H})}$ les lettres que H_α substitue à a'_1. On voit facilement que H_α permute exclusivement entre elles ces $\mathfrak{H}$ lettres, et qu'on peut leur faire correspondre une répartition

$$(8)\qquad \begin{cases} a'_1, & a''_1, & \ldots, & a_1^{(\mathfrak{H})} & \text{ou} & \alpha_1, \\ b'_1, & b''_1, & \ldots, & b_1^{(\mathfrak{H})} & \text{ou} & \beta_1, \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots, \end{cases}$$

telle que chacun des systèmes H_α, H_β, ... permute exclusivement entre elles les lettres d'un et d'un seul de ces systèmes. Si d'ailleurs un seul des systèmes de (8) coïncidait avec un des systèmes (7) les

répartitions seraient évidemment identiques, et, d'après le corollaire du théorème III, H_α ne serait pas maximum dans G. Les deux répartitions n'ont donc aucun système commun.

En considérant successivement les $\mathcal{G}$ lettres de G, on obtiendra ainsi $\frac{\mathcal{G}}{\mathfrak{S}}$ répartitions différentes. Si l'on désigne par

$$(9)\qquad \left|\begin{array}{cccc} \Sigma_1^1, & \Sigma_1^2, & \ldots, & \Sigma_1^{\frac{\mathcal{G}}{\mathfrak{S}}}, \\ \ldots, & \ldots, & \ldots, & \ldots, \\ \Sigma_{\frac{\mathcal{G}}{\mathfrak{S}}}^1, & \Sigma_{\frac{\mathcal{G}}{\mathfrak{S}}}^2, & \ldots, & \Sigma_{\frac{\mathcal{G}}{\mathfrak{S}}}^{\frac{\mathcal{G}}{\mathfrak{S}}}, \end{array}\right.$$

ces $\frac{\mathcal{G}}{\mathfrak{S}}$ répartitions,

$$\Sigma_i^1, \quad \Sigma_i^2, \quad \ldots, \quad \Sigma_i^{\frac{\mathcal{G}}{\mathfrak{S}}}$$

désignant respectivement les $\frac{\mathcal{G}}{\mathfrak{S}}$ systèmes de la $i^{\text{ième}}$ répartition, et Σ_i^j étant le système de cette répartition dont le $j^{\text{ième}}$ des groupes H_α, H_β, … permute les lettres exclusivement entre elles, les substitutions de ce $j^{\text{ième}}$ groupe seront de la forme

$$\left\{\begin{matrix}\Sigma_1^j\\ \Sigma_1^j\end{matrix}\right\}\left\{\begin{matrix}\Sigma_2^j\\ \Sigma_2^j\end{matrix}\right\}\cdots\left\{\begin{matrix}\Sigma_{\frac{\mathcal{G}}{\mathfrak{S}}}^j\\ \Sigma_{\frac{\mathcal{G}}{\mathfrak{S}}}^j\end{matrix}\right\}.$$

Une substitution de G qui transforme le $j^{\text{ième}}$ de ces groupes en le $k^{\text{ième}}$ sera de la forme

$$\left\{\begin{matrix}\Sigma_1^j\\ \Sigma_1^k\end{matrix}\right\}\left\{\begin{matrix}\Sigma_2^j\\ \Sigma_2^k\end{matrix}\right\}\cdots\left\{\begin{matrix}\Sigma_{\frac{\mathcal{G}}{\mathfrak{S}}}^j\\ \Sigma_{\frac{\mathcal{G}}{\mathfrak{S}}}^k\end{matrix}\right\}.$$

Une substitution commune à plusieurs des groupes H_α, H_β, H_γ, ... sera indifféremment d'une des formes correspondantes.

Des groupes conjoints.

Comme nous l'avons dit au début de ce Chapitre, M. Jordan a montré que les groupes transitifs, dont l'ordre égale le degré, sont conjoints deux à deux, de telle sorte que chacun d'eux soit formé par l'ensemble des substitutions échangeables à celles de l'autre.

Il a montré en même temps qu'à une répartition

$$(10) \qquad \begin{cases} a', & a'', & \ldots, & a^{(m)}, \\ b', & b'', & \ldots, & b^{(m)}, \\ \ldots, & \ldots, & \ldots, & \ldots, \end{cases}$$

admise par l'un des deux groupes G et déduite de la substitution $g = (a'a''\ldots a^{(m)})\ldots$ contenue dans ce groupe et dont l'un des cycles permutait exclusivement entre elles les lettres d'un des systèmes de cette répartition, correspondait dans l'autre groupe Γ une substitution $\gamma = (a'a''\ldots a^{(m)})(b'b''\ldots b^{(m)})\ldots$ dont chaque cycle permute exclusivement entre elles les lettres d'un système du tableau (10).

Nous avons vu d'autre part (théorème I) qu'à un groupe quelconque L contenu dans G correspondait une répartition des lettres de G, $\mathfrak{L}$ à $\mathfrak{L}$, telle que L permute exclusivement entre elles les lettres d'un au moins des systèmes de cette répartition. Nous allons voir qu'on peut établir pour le groupe L une propriété analogue à celle établie par M. Jordan pour la substitution g et qui en sera la généralisation.

En effet, soient $a', a'', \ldots, a^{(\mathfrak{L})}$ un système d'une répartition de G correspondante à L, et dont L permute les lettres exclusivement entre elles,

$$l = (a'a''\ldots a^{(m)})\ldots$$

une substitution quelconque de L. En la transformant par les substitutions de L, on voit que le système $a', a'', \ldots, a^{(\mathfrak{L})}$ est formé de $\frac{\mathfrak{L}}{m}$ systèmes de la répartition de G correspondante à l. La substitution λ

correspondante à l dans Γ et de la forme

$$\lambda = (a' a'' \ldots a^{(m)}) \ldots$$

permutera donc exclusivement entre elles les a', a'', ..., $a^{(\mathfrak{L})}$.

En considérant successivement les $\mathfrak{L}$ substitutions de L

$$\begin{pmatrix} a' \ldots \\ a' \ldots \end{pmatrix}, \quad \begin{pmatrix} a' \ldots \\ a'' \ldots \end{pmatrix}, \quad \ldots, \quad \begin{pmatrix} a' & \ldots \\ a^{(\mathfrak{L})} & \ldots \end{pmatrix},$$

et dans chacune d'elles le cycle où entre a', on trouve, dans Γ, $\mathfrak{L}$ substitutions correspondantes de la même forme respectivement, qui sont différentes, permutent exclusivement entre elles les lettres a', a'', ..., $a^{(\mathfrak{L})}$, et, par suite, forment un groupe Λ correspondant à L. Les substitutions de Λ étant échangeables à celles de G, Λ permute exclusivement entre elles les lettres de chacun des systèmes de la répartition correspondante à L pour G et dont un des systèmes est a', a'', ..., $a^{(\mathfrak{L})}$.

Réciproquement, L correspond à Λ dans G.

Les groupes formés respectivement par les substitutions opérées par L et Λ entre les lettres a', a'', ..., $a^{(\mathfrak{L})}$ sont évidemment conjoints.

Théorème XII. — *A tout groupe* L *contenu dans un groupe* G *transitif dont l'ordre égale le degré, on peut toujours faire correspondre dans le conjoint* Γ *de* G *un groupe* Λ *de même ordre que* L *et qui permute exclusivement entre elles les lettres de chacun des systèmes d'une répartition quelconque des lettres de* G *correspondante à* L; *et réciproquement.*

Si au lieu de considérer a', a'', ..., $a^{(\mathfrak{L})}$ on considère $\mathfrak{L}$ autres lettres permutées exclusivement entre elles par L, on fera correspondre à L dans Γ un groupe Λ' différent ou non de Λ. Désignons par $n'\mathfrak{L}$ l'ordre du plus grand groupe de G dont les substitutions sont permutables à L. L permute exclusivement entre elles les lettres de n' systèmes d'une répartition quelconque des lettres de G qui lui correspond. Le groupe Λ correspondant à L pour un de ces systèmes,

lui correspondra aussi pour les $n' - 1$ autres. Inversement, si Λ correspond à L pour n' systèmes de $\mathcal{L}$ lettres permutées exclusivement entre elles par les substitutions de L et de Λ, en transformant Λ et L par une substitution de Γ remplaçant une lettre d'un de ces n' systèmes par une lettre d'un autre de ces n' systèmes, on voit que ces n' systèmes font partie d'une même répartition admise par G et que G contient un groupe d'ordre $n'\mathcal{L}$ dont les substitutions sont permutables à L. Le nombre des groupes Λ, correspondant à L et différents, sera de $\frac{\mathcal{G}}{\mathcal{L}n'}$. Ces groupes seront les transformés les uns des autres par les substitutions de Γ, et $\frac{\mathcal{G}}{\mathcal{L}n'}$ sera le nombre de répartitions différentes correspondantes à L et admises par G. Des propriétés analogues et correspondantes ont lieu pour Λ.

De là résulte que pour avoir les diverses répartitions admises par G et correspondant à L, il suffit de former les divers transformés de Λ par les substitutions de Γ. Si Λ_1 est l'un d'eux et s'il permute respectivement entre elles les lettres de chacune des lignes du tableau

$$\begin{array}{cccc} a'_1, & a''_1, & \ldots, & a_1^{(\mathcal{L})}, \\ b'_1, & b''_1, & \ldots, & b_1^{(\mathcal{L})}, \\ \ldots, & \ldots, & \ldots, & \ldots, \end{array}$$

ce tableau donnera une répartition des lettres de G, $\mathcal{L}$ à $\mathcal{L}$, chaque ligne formant un système.

Si Λ est permutable aux substitutions de Γ, une seule répartition des lettres de G, $\mathcal{L}$ à $\mathcal{L}$, correspond à L, et L est permutable aux substitutions de G.

Toutes ces propriétés sont évidemment réciproques et l'on peut répéter, par rapport à L et Λ, ce qui a été montré pour Λ et L.

Si Λ est permutable aux substitutions de Γ, par suite L à celles de G, la répartition unique de Γ correspondante à Λ et la répartition unique de G correspondante à L se confondent. Réciproquement, si G et Γ admettent une répartition commune des lettres $\mathcal{L}$ à $\mathcal{L}$, et si L et Λ sont des groupes correspondants dans G et Γ, L et Λ permutent évidemment exclusivement entre elles les lettres de chacun des systèmes de la répartition commune.

On voit ainsi que si un des deux conjoints admet une propriété correspondante à un des théorèmes I, II, III, IV, l'autre admet une propriété analogue et correspondante.

Cas où les groupes correspondants L et Λ sont maxima.

Ils le seront évidemment en même temps. Si L est permutable aux substitutions de G, Λ l'est à celles de Γ et les deux répartitions correspondantes sont identiques.

Si L n'est pas permutable aux substitutions de G, Λ ne le sera pas à celles de Γ. On a vu qu'à L correspondent pour G $\frac{\mathcal{G}}{\mathcal{L}}$ répartitions en systèmes,

$$(9)\qquad \left\{\begin{matrix} \Sigma_1^1, & \Sigma_1^2, & \ldots, & \Sigma_1^{\frac{\mathcal{G}}{\mathcal{L}}}, \\ \ldots, & \ldots, & \ldots, & \ldots, \\ \Sigma_{\frac{\mathcal{G}}{\mathcal{L}}}^1, & \Sigma_{\frac{\mathcal{G}}{\mathcal{L}}}^2, & \ldots, & \Sigma_{\frac{\mathcal{G}}{\mathcal{L}}}^{\frac{\mathcal{G}}{\mathcal{L}}}, \end{matrix}\right.$$

chaque ligne de ce tableau donnant une répartition. On sait, de plus, que si $L_1, \ldots, L_i, \ldots, L_{\frac{\mathcal{G}}{\mathcal{L}}}$ sont les transformés de L par les substitutions de G, L_i permute exclusivement entre elles les lettres de chacun des systèmes composant la $i^{\text{ième}}$ colonne. A L_i correspond un groupe de Γ qui permute exclusivement entre elles les lettres de Σ_1^i, et, en transformant ce groupe Λ_1 par les substitutions de G, on voit que ses substitutions sont toutes de la forme

$$\begin{Bmatrix} \Sigma_1^1 \\ \Sigma_1^1 \end{Bmatrix} \begin{Bmatrix} \Sigma_1^2 \\ \Sigma_1^2 \end{Bmatrix} \cdots \begin{Bmatrix} \Sigma_1^{\frac{\mathcal{G}}{\mathcal{L}}} \\ \Sigma_1^{\frac{\mathcal{G}}{\mathcal{L}}} \end{Bmatrix}.$$

Les groupes de Γ correspondant à L_i étant les transformés de Λ_1 par

les substitutions de Γ, leurs substitutions sont de la forme

$$\begin{pmatrix} \Sigma_j^1 \\ \Sigma_j^1 \end{pmatrix} \begin{pmatrix} \Sigma_j^2 \\ \Sigma_j^2 \end{pmatrix} \cdots \begin{pmatrix} \Sigma_j^{\frac{\mathcal{G}}{\mathcal{L}}} \\ \Sigma_j^{\frac{\mathcal{G}}{\mathcal{L}}} \end{pmatrix},$$

pour le $j^{\text{ième}}$ Λ_j. i étant d'ailleurs quelconque, on voit que les $\frac{\mathcal{G}}{\mathcal{L}}$ groupes correspondant à L_i seront les mêmes quel que soit i. De même les $\frac{\mathcal{G}}{\mathcal{L}}$ groupes L correspondant à Λ_j seront les mêmes quel que soit j, et les transformés d'un d'entre eux par les substitutions de G. (Cette propriété n'est d'ailleurs pas particulière aux groupes L et Λ maxima.)

On voit, en résumé, que les propriétés qui existent pour G par rapport aux lignes et aux colonnes du tableau (9) existent pour Γ par rapport aux colonnes et aux lignes de ce même tableau.

Substitutions et répartitions communes à deux conjoints.

Les substitutions communes à deux conjoints G et Γ forment évidemment un groupe P d'ordre $\mathfrak{P}$ formé de toutes les substitutions de G et Γ échangeables à la fois à celles de ces deux groupes. Les répartitions des lettres de G et Γ correspondantes à P et aux groupes qu'il contient sont évidemment communes.

D'autre part, nous avons vu que la condition nécessaire et suffisante pour qu'une répartition soit commune aux deux conjoints est qu'il n'y ait dans chacun d'eux qu'un groupe correspondant L et Λ à cette répartition et permutable aux substitutions de G et Γ simultanément. Si l'on considère en particulier la répartition commune la plus générale et si L et Λ sont les groupes correspondants, ils contiendront évidemment le groupe P, à moins que G ne soit dérivé de L et d'une substitution d'ordre premier, ou dont une puissance première fait partie de L, cette substitution faisant partie de P. Dans ce cas, L et Λ seraient respectivement maxima dans G et Γ qui seraient isomorphes à deux groupes formés chacun des puissances d'une substitution

d'ordre premier entre les systèmes de la répartition commune. Ces substitutions seraient échangeables et, par suite, les deux groupes d'ordre premier isomorphes à G et Γ seraient identiques.

De plus, si l'on considère le groupe G et un groupe quelconque Λ de Γ, Λ permute exclusivement entre elles les lettres de chacun des systèmes d'une répartition admise par G. Tout groupe contenu dans G admet cette répartition. On en conclut donc que deux groupes quelconques de G et Γ, qui ne sont pas tous deux identiques à G et Γ ont toujours en commun une répartition des lettres $\mathcal{L}$ à $\mathcal{L}$, $\mathcal{L}$ étant l'ordre d'un de ces groupes arbitrairement choisi.

Groupe dérivé de deux conjoints.

Soient G et Γ les deux conjoints, P le groupe commun. L'ordre du groupe dérivé (G, Γ) est $\frac{\mathcal{G}^2}{\mathcal{P}}$ et ce groupe est transitif entre $\mathcal{G}$ lettres. Toute répartition des lettres en systèmes de non primitivité admise par (G, Γ) l'est par G et par Γ, et réciproquement. Les répartitions admises par (G, Γ) seront donc les répartitions communes à G et Γ.

Soient α, β, γ, ... les systèmes d'une des répartitions les plus générales communes; L et Λ les groupes correspondants dans G et Γ. Les deux groupes formés par les substitutions que G et Γ opèrent entre les α, β, γ, ..., G′ et Γ′ n'ont évidemment aucune répartition commune. Ces groupes sont, d'ailleurs, transitifs, d'ordre égal au degré $\frac{\mathcal{G}}{\mathcal{L}}$, formé de substitutions échangeables à celles de l'autre groupe et conjoints. Le groupe dérivé (G′, Γ′) est alors d'ordre $\frac{\mathcal{G}^2}{\mathcal{L}^2}$, de degré $\frac{\mathcal{G}}{\mathcal{L}}$ et primitif, sauf si L et Λ sont maxima dans G et Γ, auquel cas G′ et Γ′ coïncident et sont formés des puissances d'une substitution circulaire d'ordre premier.

Si donc on forme tous les groupes dérivés de la combinaison des conjoints deux à deux et si dans les groupes ainsi obtenus, on considère les substitutions opérées entre les systèmes d'une répartition maxima commune à deux conjoints, on n'obtiendra avec ces substitutions que des groupes primitifs.

Si, d'ailleurs, on remarque que les deux conjoints G′ et Γ′ qui n'ont aucune répartition commune sont forcément des groupes simples, on voit qu'il suffira, pour obtenir tous ces groupes primitifs, de considérer les conjoints qui sont simples.

D'après ce qu'on a vu précédemment, un groupe contenu dans (G', Γ') et dérivé de deux groupes contenus respectivement dans G′ et Γ′ ne sera pas primitif s'il est $< (G', \Gamma')$.

D'où les théorèmes suivants :

Théorème XIII. — *Étant donnés deux groupes transitifs dont l'ordre égale le degré et conjoints,* G *et* Γ, *si l'on forme le groupe dérivé* (G, Γ) *et l'isomorphe primitif de ce groupe comprenant les substitutions opérées par* (G, Γ) *entre les systèmes d'une répartition maxima admise par* (G, Γ), *cet isomorphe pourra toujours s'obtenir quand* G *et* Γ *sont composés, par la combinaison de deux groupes transitifs dont l'ordre égale le degré, conjoints et simples.*

Théorème XIV. — *Tout groupe* G *simple, transitif et dont l'ordre égale le degré* $\mathcal{G}$, *combiné avec son conjoint* Γ, *qui est alors simple, donne un groupe* (G, Γ) *primitif, d'ordre* $\mathcal{G}^2$, *de degré* $\mathcal{G}$, *ayant pour facteurs de composition* $\mathcal{G}$ *et* $\mathcal{G}$, *l'ordre* $\mathcal{G}$ *de* G *étant supposé non premier.*

En appliquant le théorème V, on en déduit :

Théorème XV. — *De tout groupe simple quelconque d'ordre* $\mathcal{G}$ *non premier, on déduit, par la considération de l'isomorphe transitif dont l'ordre égale le degré et de son conjoint, un groupe primitif d'ordre* $\mathcal{G}^2$, *de degré* $\mathcal{G}$, *de facteurs de composition* $\mathcal{G}$ *et* $\mathcal{G}$.

Classe de ces groupes. — Soient g une substitution quelconque de G, γ une substitution quelconque de Γ. Une substitution de (G, Γ) est de la forme $g\gamma$. Il suffit, pour avoir la classe de (G, Γ), de savoir combien $g\gamma$ peut laisser au maximum de lettres immobiles.

Soit

$$g = (a'a''\ldots a^{(m)})(b'_1 b''_1 \ldots b_1^{(m)})\ldots.$$

Pour que $g\gamma$ laisse par exemple a' immobile, il faut que

$$\gamma = (a''a'\ldots)\ldots$$

et

$$\gamma^{-1} = (a'a''\ldots a^{(m)})(b'b''\ldots b^{(m)})\ldots,$$

$$\begin{matrix} a', & a'', & \ldots, & a^{(m)}, \\ b', & b'', & \ldots, & b^{(m)}, \\ \ldots, & \ldots, & \ldots, & \ldots \end{matrix}$$

étant la répartition en systèmes correspondante à la substitution g dans le groupe G (JORDAN, *Traité des substitutions,* p. 60 et suiv.). La condition nécessaire et suffisante pour que $g\gamma$ laisse quelque lettre immobile est donc que les groupes formés des puissances des substitutions g et γ respectivement soient des groupes correspondants. Si d'ailleurs ceci a lieu, les cycles de γ^{-1} et de g où entrent des lettres laissées immobiles par $g\gamma$ seront identiques, et le nombre de lettres laissées immobiles par $g\gamma$ sera mn', n' étant le nombre de cycles identiques dans g et γ^{-1}. mn' est précisément l'ordre du plus grand groupe de G dont les substitutions sont échangeables à g; soit $\frac{\mathcal{G}}{mn'} = \chi$, la classe de la substitution $g\gamma$ sera

$$\mathcal{G} - mn' = \mathcal{G}\,\frac{\chi - 1}{\chi} = mn'(\chi - 1).$$

La classe $\mathfrak{C}$ du groupe sera la valeur minima de cette expression.

THÉORÈME. — *Aucun des groupes obtenus par les théorèmes XIV et XV n'appartient à une classe q^i, q étant premier et $i < 4$.*

Premier cas : $i = 1$. — Cela résulte facilement d'un théorème de M. Jordan [*Recherches sur les substitutions* (*Journal de Liouville,*

année 1872)]. Mais on le voit de suite, parce que

$$\mathfrak{S} = q = mn'(\chi - 1) = qn'(\chi - 1)$$

et

$$n' = 1, \qquad \chi = 2, \qquad \mathcal{G} = mn'\chi = 2q,$$

et, d'après un théorème de M. Sylow déjà cité, G ne serait pas simple.

Deuxième cas : $i = 2$. — Alors G contient une substitution d'ordre q^2 déplaçant q^2 lettres ou une substitution d'ordre q déplaçant q^2 lettres,

$$\mathfrak{S} = q^2 = mn'(\chi - 1),$$

et m est égal à q^2 ou q.

Si $m = q^2$, $n' = 1$, $\chi = 2$, $\mathcal{G} = mn'\chi = 2q^2$, et d'après le même théorème de M. Sylow, G ne serait pas simple.

Si $m = q$ ou bien $n' = q$, $\chi = 2$ et $\mathcal{G} = 2q^2$, ce qui ferait que G ne serait pas simple, ou bien $n' = 1$, $\chi = q + 1$, $\mathcal{G} = mn'\chi = q(q + 1)$: dans ce cas, G étant simple devrait être isomorphe holoédriquement à un groupe de degré $q + 1$ et d'ordre $q(q + 1)$ transitif; on sait qu'un tel groupe est composé [Jordan, *Recherches sur les substitutions* (*Journal de Liouville*, année 1872)].

Troisième cas : $i = 3$.

$$\mathfrak{S} = q^3 = mn'(\chi - 1)$$

donne m égal à q^3, q^2 ou q.

Si $m = q^3$, $n' = 1$, $\chi = 2$, $\mathcal{G} = mn'\chi = 2q^3$, et G ne serait pas simple d'après le théorème de Sylow.

Si $m = q^2$, ou bien $n' = q$, $\chi = 2$, $\mathcal{G} = 2q^3$, et G ne serait pas simple; ou bien $n' = 1$, $\chi = q + 1$, $\mathcal{G} = q^2(q + 1)$, et G serait isomorphe à un groupe transitif de degré $q + 1$, où le groupe laissant une lettre immobile et déplaçant au plus q lettres serait d'ordre q^2, ce qui est absurde.

Si $m = q$, ou bien $n' = q^2$, $\chi = 2$, $\mathfrak{g} = 2q^3$, cas qui s'écarte comme précédemment, ou bien $n' = q$, $\chi = q + 1$, $\mathfrak{g} = q^2(q + 1)$, cas qui s'écarte encore de la même façon, ou bien $n' = 1$, $\chi = q^2 + 1$, $\mathfrak{g} = q(q^2 + 1)$: $\mathfrak{g}$ est de la forme $4h + 2$, et l'on sait, d'après M. Mathieu, que G n'est pas simple. On le voit d'ailleurs en remarquant que G étant transitif et d'ordre égal au degré $4h + 2$ contient une substitution d'ordre 2 déplaçant $4h + 2$ lettres et formée de $2h + 1$ cycles de 2 lettres; G contient donc des substitutions qui ne font pas partie du groupe alterné et n'est pas simple, contrairement à l'hypothèse faite sur G.

Applications des théorèmes XIII, XIV et XV.

Nous allons appliquer ces trois théorèmes à un certain nombre de groupes, simples ou non, de façon à en déduire des groupes primitifs. Ces groupes sont :

I. Le groupe alterné de k éléments.

II. Le groupe H_n contenu dans le groupe abélien (mod p) à $2n$ indices (JORDAN, *Traité des substitutions*, p. 176 et suiv.), qui est simple si $p = 2$ et a pour facteurs de composition 2 et $\frac{\mathfrak{g}_n}{2}$, $\mathfrak{g}_n$ étant son ordre et p étant > 2.

$\mathfrak{g}_n$ est la quantité désignée par M. Jordan par Ω_n.

III. Les groupes hypoabéliens (mod 2) (même Traité, p. 205 et suiv.).

IV. Les groupes de Steiner (même Traité, p. 229 et suiv.).

V. Les groupes linéaires (mod 2) à n indices, qui sont simples (même Traité, p. 99 et suiv.).

I. — GROUPE ALTERNÉ DE k ÉLÉMENTS.

Ce groupe est simple et d'ordre $\frac{1.2\ldots k}{2} = \frac{k!}{2}$, si $k > 4$ (même Traité, p. 66). En appliquant le théorème XV, on a :

THÉORÈME. — *Si $k > 4$, en considérant le groupe transitif dont*

l'ordre égale le degré isomorphe au groupe alterné de k éléments et le combinant avec son conjoint, on obtient un groupe primitif d'ordre $\left(\frac{k!}{2}\right)^2$, *de degré* $\frac{k!}{2}$, *de facteurs de composition* $\frac{k!}{2}$ *et* $\frac{k!}{2}$.

Nous allons considérer spécialement les cas de $k = 5$, 6 ou 7, et déterminer chaque fois la classe des groupes correspondants et le nombre de lettres que peuvent déplacer leurs substitutions, c'est-à-dire les diverses valeurs de $\mathcal{G} - mn' = \mathcal{G}\frac{\chi - 1}{\chi} = mn'(\chi - 1)$.

Groupe primitif dérivé du groupe alterné entre 5 éléments.

Il contient des substitutions d'ordre 2, 3 et 5. $\mathcal{G} = 60$.

Pour $m = 2$, $g = (a_1 a_2)(a_3 a_4)$ et la substitution g est transformée en elle-même par les substitutions dérivées de g et de $(a_1 a_3)(a_2 a_4)$. D'où $n' = 2$, $\mathcal{G} - mn' = 56$.

Pour $m = 3$, $g = (a_1 a_2 a_3)$ et la substitution g est transformée en elle-même par les substitutions dérivées de g. D'où

$$n' = 1, \qquad \mathcal{G} - mn' = 57.$$

Pour $m = 5$, $g = (a_1 a_2 a_3 a_4 a_5)$ et la substitution g est transformée en elle-même par les substitutions dérivées de g. D'où

$$n' = 1, \qquad \mathcal{G} - mn' = 55.$$

Théorème. — *Le groupe transitif, dont l'ordre égale le degré et égale* 60, *dérivé du groupe alterné entre* 5 *lettres, combiné avec son conjoint, donne un groupe primitif de degré* 60, *d'ordre* $60^2 = 3600$, *de facteurs de composition* 60 *et* 60, *de classe* 55, *et ne renfermant que des substitutions déplaçant respectivement* 55, 57, 56 *et* 60 *lettres, la substitution* 1 *exceptée.*

Groupe primitif dérivé du groupe alterné entre 6 lettres.

Il contient des substitutions d'ordre 2, 3 et 5, contenues dans le groupe alterné entre 5 lettres, et de la forme

$$(a_1 a_2)(a_3 a_4), \quad (a_1 a_2 a_3), \quad (a_1 a_2 a_3 a_4 a_5),$$

et, de plus, des substitutions d'ordres 3 et 4 des formes

$$(a_1 a_2 a_3)(a_4 a_5 a_6), \quad (a_1 a_2 a_3 a_4)(a_5 a_6).$$

1° Pour les substitutions de la forme $g = (a_1 a_2)(a_3 a_4)$, la substitution g est transformée en elle-même par les substitutions dérivées de g, de $(a_1 a_3)(a_2 a_4)$ et de $(a_5 a_6)(a_1 a_2)$, et qui forment le groupe

$$1, \quad (a_1 a_2)(a_3 a_4), \quad (a_1 a_3)(a_2 a_4), \quad (a_1 a_4)(a_2 a_3),$$
$$(a_5 a_6)(a_1 a_2), \quad (a_5 a_6)(a_3 a_4), \quad (a_5 a_6)(a_1 a_4 a_2 a_3), \quad (a_5 a_6)(a_1 a_3 a_2 a_4),$$
$$\mathcal{G} - mn' = 360 - 8 = 352.$$

2° Pour les substitutions de la forme $(a_1 a_2 a_3) = g$, la substitution g est transformée en elle-même par les substitutions dérivées de

$$1, \quad (a_1 a_2 a_3), \quad (a_1 a_3 a_2),$$

formant un groupe d'ordre 3 entre 3 lettres, et de $(a_4 a_5 a_6)$, qui est telle que le groupe 1, $(a_4 a_5 a_6)$, $(a_4 a_6 a_5)$ est permutable aux substitutions précédentes. Donc

$$mn' = 9, \qquad \mathcal{G} - mn' = 360 - 9 = 351.$$

3° Pour les substitutions de la forme $(a_1 a_2 a_3 a_4 a_5)$, les substitutions du groupe d'ordre mn' sont les mêmes que celle que l'on a considérée à propos du groupe alterné entre 5 lettres,

$$mn' = 5, \qquad \mathcal{G} - mn' = 360 - 5 = 355.$$

4° Pour les substitutions de la forme $g=(a_1a_2a_3)(a_4a_5a_6)$, le groupe d'ordre mn' est formé des substitutions du groupe dérivé de $(a_1a_2a_3)$ et $(a_4a_5a_6)$,

$$mn'=9, \qquad \mathcal{G}-mn'=360-9=351.$$

5° Pour les substitutions de la forme $(a_1a_2a_3a_4)(a_5a_6)$, le groupe d'ordre mn' est dérivé de cette substitution

$$mn'=4, \qquad \mathcal{G}-mn'=360-4=356.$$

Théorème. — *Le groupe transitif dont l'ordre égale le degré et égale* 360, *dérivé du groupe alterné entre* 6 *lettres, combiné avec son conjoint, donne un groupe primitif de degré* 360, *d'ordre* $\overline{360}^2$, *de facteurs de composition* 360 *et* 360, *de classe* 351, *et ne renfermant que des substitutions déplaçant respectivement* 351, 352, 355, 356 *et* 360 *lettres, la substitution* 1 *exceptée.*

Groupe primitif dérivé du groupe alterné entre 7 lettres.

Il contient des substitutions d'ordre 2, 3, 4 et 5 contenues dans le groupe alterné entre 6 lettres, et de la forme

$$(a_1a_2)(a_3a_4), \quad (a_1a_2a_3), \quad (a_1a_2a_3a_4a_5),$$
$$(a_1a_2a_3)(a_4a_5a_6), \quad (a_1a_2a_3a_4)(a_5a_6),$$

et de plus des substitutions d'ordre 6 et 7 et de la forme

$$(a_1a_2a_3a_4a_5a_6a_7) \quad \text{et} \quad (a_1a_2)(a_3a_4)(a_5a_6a_7).$$

On trouverait respectivement pour ces substitutions les valeurs de mn' égales à

12, 36, 5, 9, 4, 7, 12

et pour $\mathcal{G}-mn'$ les valeurs

2508, 2484, 2515, 2511, 2516, 2513, 2508.

Théorème. — *Le groupe transitif dont l'ordre égale le degré et égale* 2520, *dérivé du groupe alterné entre* 7 *lettres, combiné avec son conjoint, donne un groupe primitif de degré* 2520, *d'ordre* 2520, *de facteurs de composition* 2520 *et* 2520, *de classe* 2484, *et ne renfermant que des substitutions déplaçant respectivement* 2484, 2508, 2511, 2513, 2515, 2516 *et* 2520 *lettres, la substitution* 1 *exceptée.*

Si l'on voulait continuer de la sorte, on se servirait, pour le groupe transitif dont l'ordre égale le degré dérivé du groupe alterné entre n lettres, des résultats trouvés pour les groupes transitifs dont l'ordre égale le degré dérivé des groupes alternés de moins de k lettres, comme nous l'avons fait pour les valeurs de k égales à 6 ou à 7.

II. — Groupe H_n contenu dans le groupe abélien $(\bmod p)$ à $2n$ indices.

Le groupe abélien $(\bmod p)$ à $2n$ indices, que nous désignerons par G, est défini, l'ensemble des substitutions linéaires

$$S = \left| \begin{array}{l} x_1, y_1;\ \ a_1^1 x_1 + c_1^1 y_1 + \ldots \\ \qquad\qquad + a_n^1 x_n + c_n^1 y_n,\ \ b_1^1 x_1 + d_1^1 y_1 + \ldots + b_n^1 x_n + d_n^1 y_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_n, y_n;\ \ a_1^{(n)} x_1 + \ldots + c_1^{(n)} y_1 + \ldots \\ \qquad\qquad + a_1^{(n)} x_n + c_1^{(n)} y_n,\ \ b_1^{(n)} x_1 + d_1^{(n)} y_1 + \ldots + b_n^{(n)} x_n + d_n^{(n)} y_n \end{array} \right| (\bmod p),$$

telles qu'en les effectuant simultanément pour les indices $x_1 y_1, \ldots, x_n, y_n$; et pour les indices correspondants $\xi_1, \eta_1, \ldots, \xi_n, \eta_n$, sur la fonction

$$\varphi_n = x_1 \eta_1 - \xi_1 y_1 + \ldots + x_n \eta_n - \xi_n y_n,$$

cette fonction se trouve remplacée par $m\varphi_n$, m étant un facteur numérique $(\bmod p)$.

Les substitutions abéliennes, pour lesquelles on a $m \equiv 1 (\bmod p)$, forment évidemment un groupe que nous désignerons par H_n pour le groupe abélien à $2n$ indices, son ordre étant $\mathfrak{h}_n$.

M. Jordan a montré, en particulier, pour H_n les propriétés suivantes :

L'ordre $\mathfrak{H}_n$ de H_n est

$$\mathfrak{H}_n = (p^{2n}-1)p^{2n-1}(p^{2n-2}-1)p^{2n-3}\dots p^3(p^2-1)p,$$

quel que soit p.

Si $p > 2$, les facteurs de composition de H_n sont 2 et $\frac{\mathfrak{H}_n}{2}$, les substitutions de H_n étant toutes permutables au groupe K formé de la substitution 1 et de la substitution

$$U = \begin{vmatrix} x_1, & y_1; & -x_1, & -y_1 \\ \dots, & \dots, & \dots\dots, & \dots\dots, \\ x_n, & y_n; & -x_n, & -y_n \end{vmatrix} \quad (\text{mod}\, p),$$

et les seuls groupes de H_n permutables aux substitutions de H_n étant identiques à K ou à H_n.

Si $p = 2$ et $n > 2$, H_n est simple.

Si $p = 2$ et $n = 2$, H_2 a pour facteurs de composition 2 et $\frac{\mathfrak{H}_2}{2}$.

Premier cas : $p > 2$. — Si l'on forme l'isomorphe H'_n de H_n, dont l'ordre égale $\mathfrak{H}_n$ et son conjoint H''_n, tous les deux auront en commun une répartition de leurs lettres deux à deux correspondant à K. Si l'on déduit alors leurs isomorphes I'_n et I''_n transitifs dont l'ordre égale le degré $\frac{\mathfrak{H}_n}{2}$ et qui sont formés respectivement par les substitutions opérées par H'_n et H''_n entre les systèmes de la répartition commune correspondant à K, ces groupes n'auront aucune répartition commune et seront simples ; le groupe (I'_n, I''_n) dérivé sera donc primitif et de l'ordre $\left(\frac{\mathfrak{H}_n}{2}\right)^2$.

Les substitutions de K sont échangeables à celles de H_n. Soit T une substitution de H_n, ne faisant pas partie de K ; si ω est l'ordre du plus grand groupe de H_n dont les substitutions transforment T en T ou en TU, le groupe correspondant dans I'_n sera d'ordre $\frac{\omega}{2}$. On en déduira

dans (I'_n, I''_n) des substitutions déplaçant $\frac{\mathfrak{H}_n}{2} - \frac{\omega}{2}$ lettres et le minimum de $\frac{\mathfrak{H}_n}{2} - \frac{\omega}{2}$ donnera évidemment la classe du groupe (I'_n, I''_n).

Théorème. — *Si l'on considère le groupe* H_n *formé de l'ensemble des substitutions abéliennes* $(\bmod p)$ *à* $2n$ *indices qui laissent invariable la fonction* φ_n; *si l'on forme son isomorphe transitif dont l'ordre égale le degré, et qu'on le combine avec son conjoint; si du groupe ainsi obtenu on tire les substitutions opérées par ce groupe entre les systèmes de la répartition de ses lettres deux à deux qu'il admet, ces substitutions forment un groupe primitif de degré*

$$\frac{\mathfrak{H}_n}{2} = \frac{1}{2}(p^{2n}-1)p^{2n-1}(p^{2n-2}-1)\ldots p^3(p^2-1)p,$$

d'ordre $\left(\frac{\mathfrak{H}_n}{2}\right)^2$, *de facteurs de composition* $\frac{\mathfrak{H}_n}{2}$ *et* $\frac{\mathfrak{H}_n}{2}$, *et dont les substitutions déplacent* $\frac{\mathfrak{H}_n}{2}$ *ou* $\frac{\mathfrak{H}_n}{2} - \frac{\omega}{2}$ *lettres,* ω *étant l'ordre du groupe des substitutions de* H_n *qui transforment une substitution* T *de* H_n *en* T *ou en* TU. p *est supposé* > 2.

Deuxième cas : $p = 2$. — On conclut le théorème suivant :

Théorème. — *Si l'on considère le groupe* H_n *formé de l'ensemble des substitutions abéliennes* $(\bmod 2)$, n *étant* > 2, *et si l'on forme son isomorphe transitif, dont l'ordre égale le degré, puis qu'on le combine avec son conjoint, le groupe ainsi obtenu est primitif de degré*

$$\mathfrak{H}_n = (2^{2n}-1)2^{2n-1}(2^{2n-2}-1)\ldots 2^3(2^2-1)2,$$

d'ordre $\mathfrak{H}_n^2$, *de facteurs de composition* $\mathfrak{H}_n$ *et* $\mathfrak{H}_n$.

Examen d'un cas particulier.

Nous prendrons, à titre d'exemple, pour la détermination de la classe, le cas de $n = 1$, p étant supposé > 3.

Alors H_n se confond avec le groupe des substitutions linéaires à deux indices $(\bmod p)$, dont le déterminant est $\equiv 1 \pmod p$ et

$$\mathfrak{H}_n = \mathfrak{H}_1 = (p^2 - 1)p.$$

Les groupes primitifs, qu'on en déduit par les méthodes précédentes, sont de degré $\frac{p^2-1}{2}p$ et d'ordre $\left(\frac{p^2-1}{2}p\right)^2$. Nous allons déterminer combien de lettres déplacent leurs substitutions, c'est-à-dire les quantités que nous avons désignées par m et n' antérieurement, ou simplement la quantité ω.

Une substitution quelconque de H

$$S = | x, y ; ax + cy, bx + dy | \pmod p$$

satisfait à la condition nécessaire et suffisante

$$ad - bc \equiv 1 \pmod p.$$

Soit (S) le groupe formé des puissances de S; pour savoir quel est l'ordre ω du groupe F des substitutions qui transforment S en S ou en SU, nous pouvons supposer S ramené à sa forme canonique (Jordan, *Traité des substitutions*, p. 114 et suiv.). Nous supposons également que S ne soit ni la substitution 1, ni celle qui multiplie tous les indices par $-1 \pmod p$.

La forme canonique sera

$$(10) \qquad S_1 = \begin{vmatrix} x'; & kx' \\ y'; & k'y' \end{vmatrix} \pmod p$$

ou

$$(11) \qquad S_2 = \begin{vmatrix} x'; & kx' \\ y'; & k(x'+y') \end{vmatrix} \pmod p,$$

k et k' satisfaisant à la congruence

$$(12) \quad k^2 - k(a+d) + ad - bc \equiv 0 \equiv k^2 - k(a+d) + 1 \pmod p.$$

Si (10) est la forme canonique de (S),

$$k' = k^{-1}.$$

Soit

$$\mathrm{T} = |x, y;\ f(x,y),\ f'(x,y)|$$

une substitution quelconque de H_1,

$$x' = \varphi(x,y), \qquad y' = \varphi'(x,y),$$

la transformation d'indices qui ramène S à sa forme canonique, f, f', φ, φ' étant des fonctions linéaires en x et y. T substitue à x' et y' respectivement $\varphi(f, f')$ et $\varphi'(f, f')$, et si T' est l'expression de T à l'aide des nouveaux indices x', y', le déterminant de T' est congru au déterminant de T. La substitution T est une substitution quelconque de H; nous savons que, par hypothèse, elle a son déterminant $\equiv 1 \pmod p$. Donc, si

$$\mathrm{T}' = |x', y';\ a'x' + c'y',\ b'x' + d'y'| \qquad (\mathrm{mod}\, p),$$

on a

$$a'd' - b'c' \equiv 1 \qquad (\mathrm{mod}\, p).$$

Si T' transforme S_1 en S_1 ou en $\mathrm{S}_1\mathrm{U}$

$$\mathrm{T}'^{-1}\mathrm{S}_1\mathrm{T}' = \mathrm{S}_1 \qquad \text{ou} \qquad \mathrm{T}'^{-1}\mathrm{S}_1\mathrm{T} = \mathrm{S}_1\mathrm{U}.$$

On sait, d'ailleurs, que

$$\mathrm{T}'^{-1} = |x', y';\ d'x' - c'y',\ -b'x' + a'y'| \qquad (\mathrm{mod}\, p),$$

comme on le voit facilement.

$$\mathrm{T}'^{-1}\mathrm{S}_1\mathrm{T}' = \begin{vmatrix} x';\ a'k(d'x' - c'y') + c'k^{-1}(-b'x' + a'y') \\ y';\ b'k(d'x' - c'y') + d'k^{-1}(-b'x' + a'y') \end{vmatrix} \qquad (\mathrm{mod}\, p),$$

qui sera égal à S_1 ou $\mathrm{S}_1\mathrm{U}$, si l'on a

$$(13) \qquad \begin{cases} a'd'k - b'c'k^{-1} \equiv \pm k, & b'd'(k - k^{-1}) \equiv 0; \\ a'c'(k^{-1} - k) \equiv 0, & a'd'k^{-1} - b'c'k \equiv \pm k^{-1}. \end{cases}$$

Par hypothèse, nous avons écarté le cas de $k^{-1} \equiv k$ ou $k \equiv \pm 1$

(mod p), en sorte que la deuxième et la troisième de ces congruences nous donneront, en vertu de $a'd' - b'c' \equiv 1 \pmod{p}$: soit

$$a' \equiv 0, \qquad d' \equiv 0, \qquad -b'c' \equiv 1, \qquad k^2 \equiv -1 \qquad (\mathrm{mod}\, p),$$

avec

$$T' = |x', y';\ c'y', b'x'| \qquad (\mathrm{mod}\, p);$$

soit

$$b' \equiv 0, \qquad c' \equiv 0, \qquad a'd' \equiv 1,$$

avec

$$T' = |x', y';\ a'x', d'y'| \qquad (\mathrm{mod}\, p);$$

dans ces deux cas, toutes les relations (13) sont, d'ailleurs, satisfaites.

Alors la valeur de ω pour S_1 est égale à la somme des nombres de solutions des deux congruences

$$-b'c' \equiv 1 \qquad \text{et} \qquad a'd' \equiv 1 \qquad (\mathrm{mod}\, p),$$

ou au nombre des solutions de la congruence

$$a'd' \equiv +1 \qquad (\mathrm{mod}\, p),$$

suivant que k^2 est congru ou non à $-1 \pmod{p}$.

Si k est réel, la transformation d'indices est réelle; a', b', c', d' le sont aussi, et le nombre des solutions est

$$\omega = 2(p-1) \qquad \text{ou} \qquad \omega = p - 1,$$

(le premier cas n'a lieu que pour $p = 4h + 1$, le deuxième pour $p > 5$).

Si k est imaginaire, les racines de la congruence irréductible (12) sont conjuguées et

$$k^{-1} \equiv k^p \qquad (\mathrm{mod}\, p).$$

b' et c' d'une part, a' et d' d'autre part, sont évidemment conjugués, et si b' ou a' est de la forme $\mu + \nu k$, c' ou d' est de la forme $\mu + \nu k^p$ (mod p).

ω est alors égal au nombre des solutions de la congruence

$$(\mu + \nu k)(\mu + \nu k^p) \equiv \pm 1 \qquad (\mathrm{mod}\, p),$$

ou

$$(\mu + \nu k)(\mu + \nu k^p) \equiv +1 \qquad (\mathrm{mod}\, p),$$

suivant que k^2 est congru ou non à -1 (mod$p$).

Et, si

$$\left.\begin{aligned} z &\equiv \mu + \nu k \\ z^p &\equiv \mu + \nu k^p \end{aligned}\right\} \quad (\mathrm{mod}\, p),$$

ω est égal au nombre de solutions de

$$z^{p+1} \equiv \pm 1 \qquad (\mathrm{mod}\, p)$$

ou de

$$z^{(p+1)} \equiv 1 \qquad (\mathrm{mod}\, p),$$

$2(p+1)$ divisant $p^2 - 1$, on a

$$\omega = 2(p+1) \qquad \text{ou} \qquad \omega = p - 1,$$

le premier cas n'ayant lieu que pour $p = 4h + 3$.

Si maintenant on suppose que (11) soit la forme canonique de S, k est évidemment réel, et les racines de (12) sont égales et égales à ± 1 (mod$p$).

On voit encore qu'une substitution T de H_1 exprimée à l'aide des indices x', y' sous la forme T' est telle que $a'd' - b'c' \equiv 1$ (mod$p$), comme précédemment.

Quand $k \equiv +1$ (mod$p$),

$$S_2 = \begin{vmatrix} x'; & x' \\ y'; & x' + y' \end{vmatrix} \qquad (\mathrm{mod}\, p),$$

et si

$$T'^{-1} S_2 T' = S_2,$$

(car on voit que $T'^{-1} S_2 T' = S_2 U$ est impossible),

$$T'^{-1} S_2 T' = \begin{vmatrix} x'; & a'(d'x' - c'y') + c'(d'x' - c'y' - b'x' + a'y') \\ y'; & b'(d'x' - c'y') + d'(d'x' - c'y' - b'x' + a'y') \end{vmatrix} \ (\mathrm{mod}\, p),$$

et

$$(14) \left\{ \begin{aligned} &a'd' + c'd' - b'c' \equiv 1, \qquad && b'd' + d'^2 - b'd' \equiv 1 \\ &-a'c' - c'^2 + a'c' \equiv 0, \qquad && -b'c' - d'c' + a'd' \equiv 1 \end{aligned} \right. \qquad (\mathrm{mod}\, p),$$

ce qui équivaut à

$$d' \equiv a' \equiv \pm 1, \qquad c' \equiv 0, \qquad a'd' \equiv 1 \qquad (\bmod p).$$

b' étant arbitraire et a' et d' réels, T′ sera susceptible de $2p$ valeurs : donc

$$\omega = 2p.$$

Quand $k \equiv -1$,

$$S_2 = \begin{vmatrix} x'; & -x' \\ y'; & -(x'+y') \end{vmatrix} \qquad (\bmod p),$$

$$T'^{-1}S_2T' = \begin{vmatrix} x'; & -a'(d'x'-c'y')-c'(d'x'-c'y'-b'x'+a'y') \\ y'; & -b'(d'x'-c'y')-d'(d'x'-c'y'-b'x'+a'y') \end{vmatrix} (\bmod p),$$

d'où, si $T'^{-1}S_2T' = S_2$ (car on voit que $T'^{-1}S_2T' = S_2U$ est impossible),

$$(15) \quad \left\{ \begin{array}{ll} -a'd'-c'd'+b'c' \equiv -1, & -b'd'-d'^2+b'd' \equiv -1, \\ +a'c'+c'^2-a'c' \equiv 0, & +b'c'+c'd'-a'd' \equiv -1, \end{array} \right.$$

ce qui équivaut à

$$d' \equiv a' \equiv \pm 1, \qquad c' \equiv 0, \qquad a'd' \equiv +1 \qquad (\bmod p).$$

b' étant arbitraire, et a' et d' réels, on aura encore, comme tout à l'heure, $2p$ valeurs de T′ et

$$\omega = 2p.$$

D'où le théorème :

Théorème. — *Les groupes primitifs déduits des groupes* H_1 *par le théorème de la page 40, quand* $p > 3$, *sont de degré* $\frac{p^2-1}{2}p$, *d'ordre* $\left(\frac{p^2-1}{2}p\right)^2$, *de facteurs de composition* $\frac{p^2-1}{2}p$ *et* $\frac{p^2-1}{2}p$. *On y trouvera des substitutions déplaçant* $\frac{p^2-1}{2}p$, $\frac{p^2-1}{2}p - \frac{p-1}{2}$ (*si* $p > 5$), $\frac{p^2-1}{2}p - \frac{p+1}{2}$ *ou* $p\frac{p^2-3}{2} = \frac{p^2-1}{2}p - p$ *lettres, la substitution* 1

exceptée, et aussi des substitutions déplaçant $\frac{p^2-1}{2}p-(p-1)$ *lettres, si* $p=4h+1$ *et* $\frac{p^2-1}{2}p-(p+1)$, *si* $p=4h+3$.

$p=5$ donne un groupe primitif de degré 60, d'ordre $\overline{60}^2$ dont les substitutions déplacent 60, 56, 57 ou 55 lettres. On voit facilement que ce groupe est identique à celui que nous avons déduit du groupe alterné entre 5 lettres, parce que H_1 renferme un groupe de degré $2^3=8$. Le groupe primitif de degré 60 est dérivé d'un groupe transitif H'_1 dont l'ordre égale le degré 60, et de son conjoint, H'_1 étant isomorphe à H_1 et simple. H'_1 renferme un groupe de degré 4 qui ne peut être maximum dans H'_1 que si H'_1 est isomorphe à un groupe primitif de degré 15 et d'ordre 15.4, lequel ne peut être simple quelles que soient les hypothèses faites. H'_1 renferme donc un groupe d'ordre 12 et est isomorphe au groupe alterné de 5 éléments.

$p=7$ donne un groupe de degré 168, d'ordre $\overline{168}^2$, dont les substitutions déplacent respectivement 168, 165, 164, 160 et 161 lettres. La classe est 160.

$p=11$ donne un groupe de degré 660, d'ordre $\overline{660}^2$, de classe 648, dont les substitutions déplacent 660, 655, 654, 648 et 649 lettres.

$p=13$ donne un groupe de degré 1092, d'ordre $\overline{1092}^2$, de classe 1079 et dont les substitutions déplacent 1092, 1086, 1080, 1079 et 1085 lettres.

III. — Groupes hypoabéliens.

Il y a deux groupes hypoabéliens à $2n$ indices; ils sont formés chacun des substitutions du groupe abélien (mod 2) à $2n$ indices qui satisfont à certaines conditions, n étant >2. Ils ont été définis et étudiés par M. Jordan (*Traité des substitutions*, p. 195 et suiv.) qui a montré en particulier qu'ils contenaient chacun un groupe simple I d'ordre moitié moindre.

Premier groupe hypoabélien H_0. — Il est d'ordre

$$(16)\qquad \varpi_n=(\mathfrak{P}_n-1)\,2^{2n-2}(\mathfrak{P}_{n-1}-1)\ldots(\mathfrak{P}_2-1)\,2^2(\mathfrak{P}_1-1),$$

où

$$\varphi_n = 2^{2n-1} + 2^{n-1}.$$

Il contient un groupe I_0 d'ordre $\frac{\varpi_n}{2}$ dérivé des substitutions

$$(17)\quad \begin{cases} N_{\mu\nu} = |\ldots, x_\mu, y_\mu, \ldots, x_\nu, y_\nu, \ldots;\ \ldots, x_\mu + y_\nu, y_\mu, \ldots, x_\nu + y_\mu, y_\nu, \ldots| \pmod 2, \\ Q_{\mu\nu} = |\ldots, x_\mu, y_\mu, \ldots, x_\nu, y_\nu, \ldots;\ \ldots, x_\mu + x_\nu, y_\mu, \ldots, x_\nu, y_\nu - y_\mu, \ldots| \pmod 2, \\ R_{\mu\nu} = |\ldots, x_\mu, y_\mu, \ldots, x_\nu, y_\nu, \ldots;\ \ldots, x_\mu, y_\mu - x_\nu, \ldots, x_\nu, y_\nu - x_\mu, \ldots| \pmod 2, \end{cases}$$

et de leurs transformées par les substitutions de H_0.

THÉORÈME. — *Si l'on considère l'isomorphe de* I_0 *transitif et dont l'ordre égale le degré et qu'on le combine avec son conjoint, on obtiendra un groupe primitif de degré* $\frac{\varpi_n}{2}$, *d'ordre* $\left(\frac{\varpi_n}{2}\right)^2$, *de facteurs de composition* $\frac{\varpi_n}{2}$ *et* $\frac{\varpi_n}{2}$, ϖ_n *étant donné par l'expression* (16) *donnée plus haut.*

Deuxième groupe hypoabélien H_1. — Il est d'ordre donné par

$$(18)\qquad \omega_n = 2\varphi_{n-1}(2^n - \varphi_n)\omega_{n-1}.$$

ω_n étant l'ordre du groupe hypoabélien à $2n$ indices, ω_{n-1} l'ordre du groupe hypoabélien à $2(n-1)$ indices. Il contient un groupe I_1 d'ordre $\frac{\omega_n}{2}$ dérivé des substitutions

$$N_{\mu\nu},\quad Q_{\mu\nu},\quad R_\mu \qquad \pmod 2$$

précitées, où $\mu > 1$, $\nu > 1$ et de leurs transformées par les substitutions de H_1 et I_1 est simple, comme l'a montré M. Jordan.

THÉORÈME. — *Si l'on considère l'isomorphe de* I_1 *transitif et dont l'ordre égale le degré* $\frac{\omega_n}{2}$, *et qu'on le combine avec son conjoint, on obtiendra un groupe primitif de degré* $\frac{\omega_n}{2}$, *d'ordre* $\left(\frac{\omega_n}{2}\right)^2$, *de facteurs de composition* $\frac{\omega_n}{2}$ *et* $\frac{\omega_n}{2}$, ω_n *étant donné par la formule* (18).

IV. — Groupes de Steiner.

Nous ne citons ces groupes que pour mémoire; M. Jordan les a étudiés dans son *Traité des substitutions* (p. 229 et suiv.), et il a montré qu'ils étaient : ou holoédriquement isomorphes aux groupes abéliens (mod 2), et ils donneront dès lors les mêmes groupes primitifs que ceux que nous avons obtenus par la considération de ces groupes; ou holoédriquement isomorphes aux groupes hypoabéliens H_0; et l'on retombera encore sur des groupes primitifs déjà obtenus.

V. — Groupes linéaires (mod 2) a n indices.

Ces groupes sont simples. Leur ordre est

$$(19) \qquad \Omega_n = (2^n - 1)(2^n - 2)(2^n - 2^2)\ldots(2^n - 2^{n-1}),$$

n étant supposé > 2. On sait qu'ils sont deux fois transitifs.

Théorème. — *Si l'on considère le groupe linéaire* G_n *à n indices* (mod 2) *d'ordre* Ω_n; *si l'on forme son isomorphe transitif dont l'ordre égale le degré et qu'on le combine avec son conjoint, on obtient un groupe primitif de degré* Ω_n, *d'ordre* Ω_n^2, *de facteurs de composition* Ω_n *et* Ω_n, Ω_n *étant donné par la formule* (19).

On trouve ainsi que :

Pour $n = 3$, on a un groupe primitif de degré $\Omega_3 = 168$,
Pour $n = 4$, on a un groupe primitif de degré $\Omega_4 = 20160$,
. . . .

Remarque. — Il est facile de voir que, de tous les groupes primitifs appartenant à la catégorie des groupes donnés par les théorèmes XIV et XV, aucun n'est d'un degré inférieur à 60 : sans quoi, en effet, le groupe primitif serait dérivé d'un groupe simple transitif, dont l'ordre égale le degré < 60 et de son conjoint. Or il n'existe aucun groupe simple d'ordre < 60, comme on le voit facilement à l'aide du théorème de Sylow précité ou de notre théorème IV, autre que ceux dont l'ordre est premier et ceux-là ne sont pas à considérer dans l'application des théorèmes XIV et XV.

CHAPITRE II.

DES GROUPES TRANSITIFS DE DEGRÉ N ET DE CLASSES N — 1, N — 2 OU N — 3.

PREMIÈRE PARTIE.

DES GROUPES TRANSITIFS DE CLASSE N — I ET DE DEGRÉ N.

M. Jordan a défini la classe d'un groupe comme étant égale au nombre des lettres déplacées par les substitutions de ce groupe qui déplacent le moins de lettres [*Théorèmes sur les groupes primitifs* (*Journal de Liouville,* 1871)], la substitution 1 étant exceptée. M. Netto a défini la classe d'une substitution comme étant égale au nombre des lettres déplacées par cette substitution [*Beweise und Lehrsätze über transitive Gruppen* (*Journal de Crelle,* t. 83)].

Ceci posé, soit un groupe G transitif de classe N — 1, de degré N, et d'ordre $\mathcal{G} = \mathfrak{H}N$, H étant le groupe des substitutions de G qui laissent une lettre immobile, *a* par exemple. Les substitutions de H déplacent toutes N — 1 lettres, l'unité exceptée, et permutent transitivement entre elles, $\mathfrak{H}$ à $\mathfrak{H}$, les N — 1 lettres de G autres que *a*. N — 1 est donc un multiple de $\mathfrak{H}$ et

$$N = n\mathfrak{H} + 1,$$
$$\mathcal{G} = \mathfrak{H}(n\mathfrak{H} + 1).$$

Théorème I. — *L'ordre d'un groupe transitif* G *de classe* N — 1 *et de degré* N *est de la forme*

$$\mathcal{G} = \mathfrak{H}(n\mathfrak{H} + 1)$$

avec $N = n\mathfrak{H} + 1$.

Remarque. — G renferme évidemment N groupes d'ordre $\mathfrak{H}$ qui sont les transformés du groupe H par les substitutions de G et n'ont,

2 à 2, d'autre substitution commune que l'unité. G renferme donc $N(\mathfrak{g}-1)$ substitutions de classe $N-1$, évidemment toutes régulières. De plus G renfermera alors $N-1$ substitutions déplaçant toutes les lettres, par suite de classe N et également régulières.

Si ces $N-1$ substitutions sont telles qu'on puisse toujours en trouver une qui remplace une lettre quelconque α par une autre quelconque β différente, elles forment avec l'unité un groupe dont l'ordre égale le degré N et qui est transitif. La réciproque a d'ailleurs lieu. Nous dirons que les groupes de classe $N-1$ et de degré N qui jouissent de cette propriété appartiennent à la première catégorie. Ceux qui n'en jouissent pas appartiennent à la deuxième catégorie.

Théorème II. — *Tout groupe* G′ *d'ordre* $\mathcal{G}' \equiv 0 \pmod{N}$ *et contenu dans* G *est transitif, de classe* $N-1$, *si* $\mathcal{G}' > N$ *et de la même catégorie.*

Le groupe de G′, laissant une lettre donnée immobile, est d'ordre diviseur de $\frac{\mathcal{G}'}{N}$, par suite, $\leqq \frac{\mathcal{G}'}{N} = \mathfrak{g}'$. G′ contient donc au plus $N(\mathfrak{g}'-1)$ substitutions laissant une lettre immobile, et, par suite, au moins $N-1$ substitutions déplaçant toutes les lettres. G′ contient alors toutes les substitutions de G déplaçant toutes les lettres. Les propriétés énoncées sont alors évidentes.

Corollaire. — Pour les groupes de la deuxième catégorie, le groupe G″ dérivé des substitutions de G qui déplacent toutes les lettres est transitif, de classe $N-1$, et permutable aux substitutions de G.

Car on voit facilement, à l'aide du théorème de Sylow, par exemple, que $\mathcal{G}'' \equiv 0 \pmod{N}$.

Remarque. — Le théorème précédent et, par suite, son corollaire peuvent se déduire aussi du théorème suivant, applicable à un groupe transitif quelconque.

Théorème général. — *Étant donné un groupe* G *transitif, de degré* N *et d'ordre* $\mathcal{G} = \mathfrak{g}N$, H *étant le groupe de* G *qui laisse une lettre immobile, soient* G′ *un groupe d'ordre* $\mathcal{G}' = \mathfrak{g}'N$ *contenu dans* G

et φ le plus grand commun diviseur de N *et de* $\frac{\mathfrak{h}}{\mathfrak{h}'}$: *le nombre* N′ *des lettres de* G *que* G′ *permute transitivement entre elles, une de ces lettres étant arbitrairement choisie, est un multiple de* $\frac{N}{\varphi}$.

En effet, soient p un nombre premier diviseur de N, p^n, p^q, p^r les plus hautes puissances de p qui divisent respectivement N, $\mathfrak{h}$ et $\mathfrak{h}'$. Les plus hautes puissances de p qui divisent respectivement $\mathcal{G}$ et $\mathcal{G}'$ sont p^{n+q} et p^{n+r}, en sorte que le groupe G′ contient un groupe K d'ordre p^{n+r}. Si $n + r \leqq q$, $\frac{\mathfrak{h}}{\mathfrak{h}'}$ est divisible par p^{q-r}; N par p^n, φ par p^n, et $\frac{N}{\varphi}$ n'est pas divisible par p. Si $n + r > q$, α étant la lettre laissée immobile par H, le plus grand groupe de K qui laisse α immobile est d'ordre $p^i \leqq p^q$. On voit dès lors facilement que K substitue à α p^{n+r-i} lettres, α étant d'ailleurs quelconque. La plus haute puissance de p qui divise $\frac{N}{\varphi}$ étant p^{n+r-q} qui divise p^{n+r-i}, on peut dire qu'en tout cas le nombre des lettres substituées par G′ à une lettre α arbitrairement choisie est un multiple de la plus haute puissance de p qui divise $\frac{N}{\varphi}$, p étant un diviseur premier quelconque de N, ce qui démontre le théorème.

Remarque. — Si $\frac{\mathfrak{h}}{\mathfrak{h}'}$ est premier à N, $\varphi = 1$ et G′ est transitif. C'est précisément ce qui se présente pour un groupe G′ d'ordre $\mathcal{G}' = \mathfrak{h}'N$ contenu dans un groupe G transitif de classe N — 1 et de degré N. D'où l'on déduit le théorème II.

Pour des classes inférieures à la classe N — 1 on en tire des théorèmes analogues que nous énoncerons plus loin.

Théorème III. — *Soit* $\mathcal{G} = N\mathfrak{h}$ *l'ordre d'un groupe transitif de degré* N *et de classe* N — 1 ; *si* G *n'est pas primitif,*

$$N = (n'\mathfrak{h} + 1)(n''\mathfrak{h} + 1) \qquad \text{avec} \qquad n' > 0, \qquad n'' > 0.$$

G n'étant pas primitif admet une répartition de ses lettres en systèmes de l lettres par exemple. Le groupe H de G qui laisse α immobile l'admet également; H permutant transitivement entre elles les

lettres de G, $\mathfrak{H}$ à $\mathfrak{H}$, autres que α, le système de la répartition qui comprend α, et dont les lettres sont permutées exclusivement entre elles par H, contient

$$l = n'\mathfrak{H} + 1 \qquad \text{avec} \qquad n' > 0,$$

et si

$$N = kl = n\mathfrak{H} + 1 = k(n'\mathfrak{H} + 1) \qquad \text{avec} \qquad k > 1,$$

$$k = n''\mathfrak{H} + 1 \qquad \text{avec} \qquad n'' > 0,$$

$$N = (n'\mathfrak{H} + 1)(n''\mathfrak{H} + 1) \qquad \text{avec} \qquad n' > 0, \qquad n'' > 0,$$

d'où

$$N \geqq (\mathfrak{H} + 1)^2.$$

Théorème IV. — *Soit* G *un groupe transitif de classe* N — 1 *et de degré* N. *Si l'on peut trouver dans* G *un groupe* M *ne contenant avec l'unité que des substitutions qui déplacent toutes les lettres, et permutable aux substitutions de* G *qui déplacent toutes les lettres, ou bien* $\mathfrak{M}$ *ne sera pas divisible par tous les facteurs premiers de* N *et* G *ne sera pas primitif, ou bien* $\mathfrak{M}$ *étant divisible par tous ces facteurs* G *n'est primitif que s'il appartient à la première catégorie.*

$\mathfrak{M}$ divise évidemment N. Si M est permutable aux substitutions de G, G n'est pas primitif; s'il ne l'est pas, soit M' un de ses transformés par les substitutions de G. M est évidemment permutable aux substitutions de M', et M' à celles de M. Si P est le groupe commun à M et M', (M, M') est d'ordre $\frac{\mathfrak{M}^2}{\mathfrak{P}}$ et jouit évidemment des mêmes propriétés que M. L'ordre $\frac{\mathfrak{M}^2}{\mathfrak{P}}$ de (M, M') n'admet d'ailleurs aucun autre diviseur premier que ceux de $\mathfrak{M}$.

En raisonnant alors sur (M, M') comme nous l'avons fait sur M, et continuant, on voit que, si le groupe obtenu n'est pas permutable aux substitutions de G, il est toujours possible d'en trouver un plus grand, n'admettant pas d'autres diviseurs premiers que ceux de $\mathfrak{M}$ et ne contenant avec l'unité que des substitutions qui déplacent toutes les lettres. On finira donc toujours par trouver un groupe permutable aux substitutions de G. Si $\mathfrak{M}$ n'est pas divisible par tous les facteurs premiers de N, ce groupe ne sera pas transitif et G ne sera pas primitif.

Si $\mathfrak{M}$ est divisible par tous les facteurs premiers de N, ou bien le groupe obtenu ne sera pas transitif et G ne sera pas primitif, ou bien le groupe obtenu sera transitif et de degré et d'ordre N, auquel cas il pourra être primitif, mais appartiendra à la première catégorie.

Corollaire. — Dans un groupe primitif G, de la deuxième catégorie, le groupe G′ transitif dérivé des substitutions qui déplacent toutes les lettres ne peut être primitif que s'il est simple. $\mathcal{G}'$ est alors facteur de composition de G.

Car G′ étant primitif ses substitutions ne peuvent être permutables qu'à un groupe transitif contenu dans G′. Ce groupe contiendrait toutes les substitutions de G′ qui déplacent toutes les lettres, puisque G et G′ appartiennent à la classe $N-1$, et il coïnciderait avec G′.

Théorème V. — *Pour les groupes primitifs de la première catégorie* $N=p^m$, *p étant premier; par suite, ces groupes sont linéaires.*

En effet, soit $N=\rho p^m$ avec $\rho\neq 1$ et $\rho \not\equiv 0 \pmod p$, et soit un groupe G primitif de classe $N-1$ et de degré N; soit K le groupe d'ordre N comprenant les substitutions qui déplacent toutes les lettres. D'après Sylow, $\mathfrak{N}=N=\rho p^m = p^m \nu(np+1)$ K, par suite G renfermant $np+1$ groupes d'ordre p^m. Donc

$$\mathcal{G}=\mathfrak{H}N=p^m\nu'(np+1)=p^m\nu\mathfrak{H}(np+1).$$

G renferme un groupe L d'ordre $p^m\nu\mathfrak{H}=p^m\nu'=\mathfrak{L}$ avec $p^m\nu-1$ substitutions déplaçant toutes les lettres. Par un raisonnement analogue à celui des pages 68 et 69, on voit que, si L renferme $\mathfrak{M}$ substitutions laissant une lettre arbitraire immobile, il renferme

$$\mathfrak{L}-(\mathfrak{M}-1)\frac{\mathfrak{L}}{\mathfrak{M}}-1=\frac{\mathfrak{L}}{\mathfrak{M}}-1$$

substitutions déplaçant toutes les lettres, ce qui exige $\mathfrak{M}=\mathfrak{H}$. Le groupe H, formé des substitutions de G qui laissent une lettre arbi-

traire immobile ne serait pas maximum dans G et G ne serait pas primitif.

On en conclut que les groupes primitifs de la première catégorie sont de degré $N = p^m$; donc, d'après une propriété que nous allons établir, ces groupes sont linéaires.

Examen de quelques valeurs particulières du degré N.

I. $N = p^m$ (p ÉTANT UN NOMBRE PREMIER).

D'après le théorème de Sylow, le groupe G renferme un groupe d'ordre p^m formé des substitutions qui déplacent toutes les lettres et de la substitution 1. Les groupes transitifs de classe $p^m - 1$ et de degré p^m appartiennent donc à la première catégorie. De plus, ils ne peuvent être primitifs que s'ils sont linéaires.

En effet, soit K le groupe d'ordre p^m; il y a dans ce groupe au moins une substitution autre que 1, échangeable à toutes les substitutions de K : soit p^i l'ordre du plus grand groupe de K, K′, dont les substitutions sont échangeables à toutes celles de K, et supposons $i < m$. Les substitutions de G ne peuvent être permutables à K′, sans quoi G ne serait pas primitif. L'un des groupes transformés de K′ au moins sera donc un groupe K″ différent de K′ et dont les substitutions seront encore toutes échangeables à celles de K, puisque K est permutable aux substitutions de G. Or, par hypothèse, K′ contient toutes les substitutions de K échangeables à celle de K. On est donc conduit à une contradiction, sauf si $i = m$. Dans ce cas, on sait, d'après M. Jordan (*Traité des substitutions*, p. 291 et 398), que les substitutions de K peuvent être représentées par les substitutions

$$| x_1, x_2, \ldots, x_m; x_1 + \alpha_1, x_2 + \alpha_2, \ldots, x_m + \alpha_m | \qquad (\text{mod}\, p),$$

$\alpha_1, \alpha_2, \ldots, \alpha_m$ prenant toutes les valeurs possibles (mod p), et que le groupe G est linéaire, car si un groupe d'ordre p^i ne contient que des substitutions d'ordre p échangeables à celles de K, de ce groupe et d'une substitution d'un de ses transformés, on tire un groupe d'ordre p^{i+1} ne contenant que des substitutions d'ordre p échangeables à celles de K, etc.

Si $N = p^m$, *le groupe* K *est formé de substitutions d'ordre premier p échangeables;* G *appartient à la première catégorie et est linéaire s'il est primitif.*

II. $N = 4h + 2$.

$\mathfrak{H}$ est impair et $\mathcal{G} = \mathfrak{H} N = 4h' + 2$. On sait, et d'ailleurs on voit facilement, par la considération du groupe transitif dont l'ordre égale le degré isomorphe à G, que G renferme un groupe G' d'ordre $\frac{\mathcal{G}}{2}$ permutable à ses substitutions et qui n'est pas transitif. Donc G ne peut être primitif.

Si le degré N *est de la forme* $4 + 2$, G *ne peut être primitif.*

III. $N = n\mathfrak{H} + 1$ AVEC $n < 11$.

En général, soit g une des $N - 1$ substitutions de G déplaçant toutes les lettres; les substitutions échangeables à g forment un groupe d'ordre φ et déplacent toutes les lettres : g a donc $\frac{\mathcal{G}}{\varphi}$ transformées qui déplacent toutes les lettres.

Soit g' une substitution différente des $\frac{\mathcal{G}}{\varphi}$ transformées de g : elle donne de même $\frac{\mathcal{G}}{\varphi'}$ transformées différentes et différentes des précédentes; et ainsi de suite. D'où

$$\frac{\mathcal{G}}{\varphi} + \frac{\mathcal{G}}{\varphi'} + \ldots = \mathcal{G} \sum \frac{1}{\varphi} = N - 1$$

ou

$$N \sum \frac{1}{\varphi} = \frac{N-1}{\mathfrak{H}} = n.$$

Si une seule des valeurs φ, φ', ... est égale à N, G appartient à la première catégorie et, par suite, est linéaire.

1° Or pour $n \leqq 3$, ou bien une valeur φ est égale à N, ou bien les substitutions qui déplacent toutes les lettres sont toutes transformées d'une d'entre elles, par suite, toutes d'ordre premier, ce qui exige $N = p^m$, p étant premier. Ces groupes sont donc linéaires, et l'on ob-

tient, en particulier, le résultat trouvé par M. Jordan pour $n = 1$ [*Recherches sur les substitutions* (*Journal de Liouville;* 1872.])

2° $n = 4$ ou 6. — On voit encore, ou que G appartient à la première catégorie, une des valeurs φ, φ', ... étant égale à N, ou que les substitutions déplaçant toutes les lettres sont toutes transformées d'une d'entre elles, ou que les quantités φ, φ', ... sont au nombre de 2, $\varphi = \frac{N}{2}$, $\varphi' = \frac{N}{2}$. N est divisible par 2 et le groupe L des substitutions échangeables à une substitution d'ordre 2 est d'ordre $\frac{N}{2}$ quelle que soit cette substitution. Mais, d'après le théorème de Sylow, on pourrait toujours la choisir de façon qu'elle soit échangeable à celles d'un groupe d'ordre 2^ρ, 2^ρ étant la plus haute puissance de 2 qui divise $\mathcal{G}$ ou N, et ce groupe serait alors contenu dans L, ce qui est absurde. L'hypothèse $\varphi = \frac{N}{2}$, $\varphi' = \frac{N}{2}$ conduit donc à une contradiction.

Donc les groupes G pour lesquels $n = 4$ sont linéaires.

Le cas de $n = 6$ se traite de la même façon et conduit aux mêmes conclusions.

3° $n = 5$. — En raisonnant de la même façon on voit encore que $\varphi = \frac{N}{2}$, $\varphi' = \frac{N}{3}$ à moins que G ne soit linéaire. Si donc G n'est pas linéaire, il y a $\frac{N}{2}$ substitutions d'ordre 3 déplaçant toutes les lettres et transformées d'une seule d'entre elles par les substitutions de G et $\frac{N}{3}$, substitutions d'ordre 2 ayant les mêmes propriétés. Donc $N = 2^\alpha 3^\beta$ et $\alpha > 1$. On a également $\beta > 1$, car l'hypothèse $\beta = 1$ montre, d'une part, qu'on a des substitutions d'ordre 2, échangeables à une d'ordre 3, et, d'autre part, qu'on n'en a jamais.

On écarte facilement le cas où $N = 2^\alpha 3^\beta$ avec $\alpha > 1$, $\beta > 1$, qui exigerait l'existence de substitutions d'ordre 6 déplaçant toutes les lettres.

Par des raisonnements analogues on voit que *si* $n < 11$, G *ne peut être primitif que s'il est linéaire et de degré* p^m (*p étant premier*).

IV. $N = n\mathfrak{z} + 1$. N n'admettant aucun diviseur $< n$ autre que l'unité.

Nous avons vu tout à l'heure que

$$\varphi = \frac{n\mathfrak{z} + 1}{l},$$

l étant $\leqq n$. Dans ce cas, on a forcément $l = 1$ et $\varphi = n\mathfrak{z} + 1$. Les substitutions qui déplacent toutes les lettres sont toutes échangeables et forment un groupe K.

Dans ce cas, les substitutions qui déplacent toutes les lettres sont échangeables et forment un groupe K. G *ne peut être primitif que si* $n\mathfrak{z} + 1 = N = p^m$. G *appartient à la première catégorie et est linéaire, s'il est primitif.*

V. $N = p^\alpha + 1$ (p étant un nombre premier > 2).

Alors $\mathfrak{z} = p^\beta$ et nous pouvons supposer $\beta < \alpha$, le cas de $\beta = \alpha$ rentrant dans un des cas déjà examinés

$$\mathcal{G} = p^\beta(p^\alpha + 1).$$

Si $\alpha = 2\alpha'$, $p = 4h \pm 1$, on a

$$\mathcal{G} = 4k + 2.$$

Nous avons vu qu'alors G n'est pas primitif.

Si $\alpha = 2\alpha' + 1$, $p = 4h + 1$, on a encore

$$\mathcal{G} = 4k + 2$$

et G n'est pas primitif.

Si $N = p^\alpha + 1$, $\mathcal{G} = p^\beta(p^\alpha + 1)$ avec $\alpha \geqq \beta$, G ne peut être primitif que si α est impair et p de la forme $4h - 1$.

Si $\alpha = 2$ et G non primitif $\mathcal{G} = p^\beta(p^2 + 1)$ ne satisfait pas au théorème III. Donc :

Théorème. — *Parmi les groupes transitifs de classe* N — 1 *et de*

degré N : 1° *il n'en existe aucun de classe* p^2; 2° *il n'en existe aucun de classe* $p^{2\alpha'}$ *qui soit primitif;* 3° *il n'en existe aucun de classe* $p^{2\alpha'+1}$ *qui soit primitif si* $p = 4h + 1$; *p étant un nombre premier impair.*

VI. — $N = pp_1$, p ET p_1 ÉTANT DES NOMBRES PREMIERS DIFFÉRENTS.

G renferme une substitution S d'ordre p déplaçant toutes les lettres et une substitution S_1 d'ordre p_1 déplaçant aussi toutes les lettres. Leurs puissances forment des groupes d'ordre p et p_1 que nous désignerons respectivement par (S) et (S_1). Si (S) est permutable à S_1, ou (S_1) à S, G appartient évidemment à la première catégorie. Sinon on voit par transformation qu'on aurait au moins $(p_1 - 1)p$ substitutions d'ordre p_1 et $(p - 1)p_1$ substitutions d'ordre p, déplaçant toutes les lettres, d'où

$$N - 1 = pp_1 - 1 \geqq (p - 1)p_1 + (p_1 - 1)p$$

ou

$$0 \geqq (p - 1)(p_1 - 1),$$

ce qui est absurde.

G appartient donc à la première catégorie.

Il renferme alors un groupe K d'ordre pp_1, et si, par exemple, $p > p_1$, ce groupe ne renfermera qu'une substitution S d'ordre p et ses puissances.

G n'est donc pas primitif.

En résumé : *si* $N = pp_1$, G *n'est pas primitif, et il appartient à la première catégorie.*

VII. — $N = p^2 p_1$, p ET p_1 ÉTANT DES NOMBRES PREMIERS DIFFÉRENTS.

G *appartient à la première catégorie.*

En effet, si ceci n'a pas lieu, deux cas peuvent se présenter :

1° Un des groupes d'ordre p^2 contenu dans G donnera, par transformations successives par une substitution de G d'ordre p_1 des groupes d'ordre p^2 en nombre p_1, n'ayant, deux à deux en commun,

que la substitution 1. Dans ce cas, il n'y aurait que

$$p^2p_1 - 1 - (p^2 - 1)p_1 = p_1 - 1$$

substitutions d'ordre p_1, et G appartiendrait évidemment à la première catégorie, ce qu'on ne suppose pas.

2° Un des groupes d'ordre p^2 contenu dans G donnera, par les mêmes transformations des groupes d'ordre p^2 ayant deux à deux quelque substitution commune autre que l'unité. Soient deux de ces groupes ayant en commun une substitution d'ordre p et ses puissances; ils n'en auront pas d'autres communes, sans quoi ils coïncideraient et G appartiendrait à la première catégorie. Alors le groupe dérivé de ces deux groupes a ses substitutions échangeables à l'une d'entre elles; il ne peut contenir que des substitutions qui déplacent toutes les lettres et est d'ordre $> p^2$. Il est donc d'ordre p^2p_1.

On est donc toujours conduit à une contradiction, si l'on suppose que G n'appartienne pas à la première catégorie.

G *n'est pas primitif.*

Nous venons de voir qu'il renferme un groupe K d'ordre p^2p_1 entre les substitutions qui déplacent toutes les lettres. Si $p > p_1$, on sait, d'après Sylow, que K et, par suite, G renferment un groupe unique d'ordre p^2 permutable à leurs substitutions, et G n'est pas primitif. Si $p < p_1$, on a encore, d'après Sylow, un groupe unique d'ordre p_1 permutable aux substitutions de G, sauf le cas où $p^2 = np_1 + 1$, ce qui entraîne $p_1 = p + 1$, $p = 2$, $p_1 = 3$, $N = 12$. Ce cas particulier doit être écarté, d'après ce qu'on a vu antérieurement, parce que $N - 1 = 11$.

VIII. — $N = p^2p_1^2$ (p ET p_1 ÉTANT DES NOMBRES PREMIERS DIFFÉRENTS).

On peut évidemment supposer, par exemple, $p_1 > p$. G contient un groupe P_2 d'ordre p^2 et un P'_2 d'ordre p_1^2. P_2 ne peut être tranformé par les substitutions de P'_2 en p_1^2 groupes entièrement différents, sans quoi G contiendrait un groupe unique P'_2 d'ordre p_1^2 permutable à ses substitutions, et G appartiendrait à la première catégorie et ne serait

pas primitif. Si l'on écarte ce cas, ou bien les groupes transformés, en nombre p_1^2 et différents ont, deux à deux, des substitutions communes autres que l'unité, ou bien le nombre des groupes transformés n'est que de p_1, ou bien il n'est que de 1 :

1° Deux groupes d'ordre p^2 auront une, par suite $p-1$ substitutions communes autres que l'unité. Le groupe dérivé de ces deux groupes est d'ordre $> p^2$ et contient une substitution d'ordre p échangeable à toutes ses substitutions : s'il est d'ordre $p^2 p_1^2$, G ne sera pas primitif (théorème IV) et appartiendra à la première catégorie; s'il est d'ordre $p^2 p_1$, il ne contiendra, d'après le théorème de Sylow, qu'un groupe d'ordre p_1 permutable à ses substitutions, sauf si $p^2 = ap_1 + 1$, $p_1 = p + 1$, $p = 2$, $p_1 = 3$, $N = 36$, cas que nous examinerons tout à l'heure. Ce groupe d'ordre p_1 est, d'ailleurs, contenu dans un groupe d'ordre p_1^2 dont les substitutions lui sont permutables. En combinant le groupe d'ordre $p^2 p_1$ et celui d'ordre p_1^2, on obtient un groupe d'ordre multiple de N qui contient par suite toutes les substitutions de G qui déplacent toutes les lettres et dont les substitutions sont permutables à un groupe d'ordre p_1 qu'il renferme. Alors, d'après le théorème IV, G n'est pas primitif.

2° Il existera évidemment un groupe d'ordre $p^2 p_1$; en raisonnant dessus comme précédemment, on voit que G n'est pas primitif, sauf le cas de $N = 36$.

3° G appartient à la première catégorie et n'est pas primitif.

Il nous reste à examiner le cas de $N = 36$: $\mathfrak{z} = 5$ ou $\mathfrak{z} = 7$. G renferme un groupe J d'ordre 9 et, d'après le théorème de Sylow, il ne peut renfermer de groupe d'ordre 5×9 ou 7×9. Une substitution d'ordre 5 ou 7 et ses puissances transforment donc J en des groupes différents. S'ils n'ont pas deux à deux quelque substitution commune, on aurait au moins $5 \times 8 = 40$ ou $7 \times 8 = 56$ substitutions déplaçant toutes les lettres, ce qui est absurde. Soient J' et J'' deux de ces groupes ayant une substitution commune d'ordre 3. Le groupe (J', J'') dérivé de ces deux groupes contiendra une substitution d'ordre 3 échangeable à toutes les siennes; il sera donc d'ordre 36 ou 18. S'il est d'ordre 36, G n'est pas primitif et appartient à la première catégorie (théorème IV). S'il est d'ordre 18, il ne renfermerait, d'après le théorème de Sylow, qu'un seul groupe d'ordre 9, ce qui est absurde

par hypothèse. On voit donc que, pour $N = 36$, G ne peut être primitif, et n'appartient pas à la deuxième catégorie.

Donc, si $N = p^2 p_1^2$, G *n'est pas primitif.*

IX.—$N = p_1 p_2 p_3$ (p_1, p_2, p_3 ÉTANT DES NOMBRES PREMIERS DIFFÉRENTS).

Nous pouvons évidemment supposer *a priori* que p_1 soit le plus petit de ces trois nombres premiers.

G *n'est pas primitif et appartient à la première catégorie.*

En effet, soit P_i un groupe formé des puissances d'une substitution d'ordre p_i (i prenant une des valeurs 1, 2 ou 3). D'après le théorème de Sylow, si un groupe P_1 n'est pas permutable à une substitution d'ordre p_2, ou à une d'ordre p_3, on en déduit par transformation par les substitutions de G un nombre de groupes P_1 différents qui est un multiple de p_2 et de p_3, par suite de $p_2 p_3$; on aurait ainsi au moins $p_2 p_3 (p_1 - 1)$ substitutions d'ordre p_1 et il existerait dans G un groupe d'ordre $p_2 p_3$ permutable aux substitutions de G. G appartiendrait donc à la première catégorie et ne serait pas primitif. Écartons ce cas : un groupe P_1 sera toujours permutable aux substitutions d'un groupe P_2 ou P_3 : supposons que P_1 soit permutable aux substitutions de P_2: d'après le théorème de Sylow, le groupe (P_1, P_2) d'ordre $p_1 p_2$ est formé de substitutions échangeables. Transformant ce groupe (P_1, P_2) par les substitutions d'un groupe P_3, on obtient, ou bien un groupe (P_1, P_2), auquel cas G appartient à la première catégorie et n'est pas primitif, ou bien p_3 groupes transformés de (P_1, P_2) et n'ayant en commun que la substitution 1, auquel cas G appartient encore à la première catégorie et n'est pas primitif, ou bien p_3 groupes transformés de (P_1, P_2), deux d'entre eux ayant en commun une substitution d'ordre p_1 ou p_2 : cette substitution commune est évidemment échangeable aux substitutions du groupe dérivé qui est d'ordre $> p_1 p_2$, par suite d'ordre $p_1 p_2 p_3$. G appartient donc encore à la première catégorie et n'est pas primitif.

X. — $N = p_1 p^3$ (p ET p_1 ÉTANT DES NOMBRES PREMIERS DIFFÉRENTS).

Si G est primitif, il n'appartient évidemment pas à la première catégorie :

1° Soit $p_1 < p$. Étant donné un groupe P_1 formé des puissances d'une substitution d'ordre p_1, il y a dans G des substitutions d'un groupe d'ordre p^3 qui sont permutables à P_1, sans quoi G ne serait pas primitif et appartiendrait à la première catégorie, comme on le voit facilement. Ces substitutions forment avec P_1 un groupe d'ordre $p_1 p^2$ ou $p_1 p$. Si c'est un groupe d'ordre $p_1 p^2$, la condition $p_1 < p$ montre que ce groupe est formé de substitutions échangeables; si c'est un groupe d'ordre $p_1 p$, il est formé de substitutions échangeables et la substitution d'ordre p qu'il contient fait partie d'un groupe d'ordre p^2. En combinant ce groupe d'ordre $p_1 p$ et ce groupe d'ordre p^2, on a ou un groupe d'ordre $p_1 p^3$, auquel cas G n'est pas primitif et appartient à la première catégorie, ou un groupe d'ordre $p_1 p^2$ dont les substitutions sont permutables à un groupe d'ordre p^2.

Nous arrivons donc à cette conclusion, que si G est primitif, N étant égal à $p_1 p^3$ et p_1 étant $< p$, G renferme un groupe d'ordre $p_1 p^2$, dont les substitutions sont permutables à un groupe qui est un groupe d'ordre p^2 et ce groupe d'ordre p^2 fait partie d'un groupe d'ordre p^3 aux substitutions duquel il est permutable. Combinant ce groupe d'ordre $p_1 p^2$ et ce groupe d'ordre p^3, on obtient un groupe d'ordre multiple de $p_1 p^3$, renfermant toutes les substitutions de G qui déplacent toutes les lettres et contenant un groupe d'ordre p^2 permutable à ses substitutions. D'après le théorème IV, G n'est pas primitif.

Si donc $N = p_1 p^3$ *et* $p_1 < p$, G *n'est pas primitif.*

2° Soit $p_1 > p$. Étant donné un groupe P_3 d'ordre p^3 contenu dans G, les transformés de P_3 par les puissances d'une substitution d'ordre p_1 ne seront formés de substitutions entièrement différentes (la substitution 1 mise à part) que si G n'est pas primitif et appartient à la première catégorie. Deux de ces groupes transformés auront donc en commun un groupe P_2 d'ordre p^2 ou un groupe P_1 d'ordre p. Examinons successivement ces deux cas.

Premier cas. — Deux groupes transformés P'_3, P''_3 d'ordre p^3 ont en commun un groupe P_2 d'ordre p^2. P'_3 renferme évidemment un groupe d'ordre p^i avec $i = 1$ ou 2 aux substitutions duquel est permutable le groupe Q des puissances de la substitution d'ordre p_1 considéré, sans quoi G ne serait pas primitif et appartiendrait à la première catégorie. P''_3 renferme aussi un groupe d'ordre p^i transformé du précédent et jouissant des mêmes propriétés. Si ces deux groupes d'ordre p^i sont différents, le résultat de leur combinaison, contenu dans le groupe (P'_3, P''_3), qui est formé de substitutions permutables au groupe P_2, est d'ordre $p_1 p^i$, et, d'après le théorème IV, G n'est pas primitif. Si ces deux groupes d'ordre p^i sont identiques, ils sont contenus dans P_2 et formés de substitutions échangeables à celles de Q.

Si $i = 2$, (P'_3, Q) est d'ordre multiple de $p_1 p^3$ et contient un groupe P_2 d'ordre p^2 permutable à ses substitutions. Si $i = 1$, (Q, P_2) contient une substitution d'ordre p échangeable à ses substitutions; dès lors l'ordre de (Q, P_2) est $p_1 p^3$ ou $p_1 p^2$: quand c'est $p_1 p^3$, G n'est pas primitif; quand c'est $p_1 p^2$, on voit, sauf pour $p_1 = 3$, $p = 2$, $N = p_1 p^3 = 24$, que $p_1 > p$ exigerait Q permutable aux substitutions de P_2, contrairement à l'hypothèse. Dans le premier cas, G n'est donc pas primitif.

Deuxième cas. — Deux groupes transformés quelconques P'_3, P''_3 n'ont pas plus de p substitutions communes. Il y a toujours dans P'_3 des substitutions formant un groupe d'ordre p^i et permutables au groupe Q et i est égal à 1 ou 2. Ces substitutions forment avec Q un groupe d'ordre $p^i p_1$: si $p_1 \not\equiv 1 \pmod{p}$, ce groupe est formé de substitutions échangeables, d'après le théorème de Sylow, et dès lors $i = 1$. On déduira facilement de ce groupe d'ordre pp_1 par l'adjonction d'une substitution d'ordre p un groupe d'ordre $p^2 p_1$ ou $p^3 p_1$ et finalement un groupe d'ordre $p^3 p_1$ renfermant un groupe plus petit, permutable à ses substitutions : G ne serait donc pas primitif, d'après le théorème IV; la seule exception possible reste donc le cas de $p_1 \equiv 1 \pmod{p}$.

Supposons donc $p_1 = ap + 1$.

D'après le théorème de Sylow, le nombre des groupes d'ordre p_1 renfermés dans G est égal à $a_1 p_1 + 1$. Ce nombre est, d'ailleurs, un multiple de p, sans quoi G ne serait pas primitif et appartiendrait à la

première catégorie. Donc

$$a_1 p_1 + 1 \equiv 0 \pmod{p} \quad \text{avec} \quad a_1 \geqq 1$$

ou

$$a_1(ap + 1) + 1 \equiv 0 \pmod{p},$$
$$a_1 \geqq p - 1.$$

Le nombre des substitutions d'ordre p_1 renfermées dans G sera donc, au minimum, $[(p-1)p_1+1](p_1-1)=\lambda$, et cette quantité sera évidemment $\leqq p_1 p^3 - p^3$, ce qui donnera

$$(6) \qquad (p-1)p_1 + 1 \leqq p^3.$$

Si, d'autre part, nous comptons le nombre minimum de substitutions différentes et d'ordre diviseur de p^3 données par P'_3, et les groupes transformés par les p_1 substitutions de Q, groupes que nous désignerons par

$$P'_3, \quad P''_3, \quad \ldots, \quad P_3^{(p_1)},$$

nous voyons que

P'_3 donne $p^3 - 1$ substitutions différentes;
P''_3 donne $p^3 - (p-1) - 1$ substitutions différentes et différentes des précédentes au moins;
....,
$P_3^{(i)}$ donne $p^3 - (i-1)(p-1) - 1$ substitutions différentes et différentes des précédentes au moins;
....,
$P_3^{(p_1)}$ donne $p^3 - (p_1-1)(p-1) - 1$ substitutions différentes et différentes des précédentes au moins;

puisque $P_3^{(i)}$ a, au plus, $p - 1$ substitutions communes, la substitution 1 mise à part, avec chacun des $i - 1$ groupes qui le précédent, et que $p^3 - (p_1-1)(p-1) - 1 > 0$ d'après l'inégalité (6) : en sorte que nous avons, au minimum,

$$\mu = p_1 p^3 - (p-1)\frac{p_1-1}{2}p_1 - p_1 \qquad \text{substitutions,}$$

dont l'ordre divise p^2. Il est, dès lors, évident qu'il faudrait

$$p_1 p^2 > \lambda + \mu$$

ou

$$p_1 p_2 > p_1 p_2 - (p-1)\frac{p_1 - 1}{2} p_1 - p_1 + (p-1)(p_1 - 1) p_1 + p_1 - 1,$$

ou enfin

$$(p-1)\frac{p_1 - 1}{2} p_1 - 1 < 0,$$

ce qui n'a pas lieu et l'exception que nous avons considérée ne peut avoir lieu. Donc

Si $N = p_1 p^2$ *et* $p_1 > p$, G *n'est pas primitif.*

Le cas de $N = 24$, que nous avions mis à part, ne peut évidemment se présenter, puisque $N - 1 = 23$ est un nombre premier et que 24 n'est pas de la forme 2^m.

Théorème. — *Un groupe* G *de classe* $N - 1$ *et de degré* N *transitif appartient à la première catégorie si* $\mathcal{G} = 2N$ *ou* $\mathcal{G} = 3N$.

En effet, supposons que G appartienne à la deuxième catégorie et soient $a_1, a_2, \ldots, a_N$ les lettres de G, H_{a_1} le groupe de G qui laisse a_1 immobile, d'ordre $\mathfrak{H}_{a_1} = \frac{\mathcal{G}}{N} \cdot a_2$ peut toujours être choisi de façon que toutes les substitutions $(a_1 a_2 \ldots)\ldots$ de G laissent une lettre immobile. Soient $T_1, T_2, \ldots, T_{\mathfrak{H}_{a_1}}$ les substitutions de la forme $(a_1 a_2 \ldots)\ldots$. Les substitutions de H_{a_1} seront évidemment

(1) $\quad 1, \quad T_1 T_2^{-1}, \quad \ldots, \quad T_1 T_{\mathfrak{H}_{a_1}}^{-1}; \qquad \mathfrak{H}_{a_1} = 2 \qquad$ ou $\qquad \mathfrak{H}_{a_1} = 3$

ou

(2) $\qquad T_2 T_1^{-1}, \quad 1, \quad \ldots, \quad T_2 T_{\mathfrak{H}_{a_1}}^{-1}.$

Les substitutions (1) étant différentes, les substitutions (2) également, on aura

$$T_1 T_2^{-1} = T_2 T_i^{-1}.$$

Si $i = 1$,

$$T_1 = (a_1 a_2 \ldots a_{j_1}) \ldots,$$
$$T_2 = (a_1 a_2 \ldots a_{j_2}) \ldots,$$

on a

$$T_1 T_2^{-1} = (a_1)(a_{j_1} a_{j_2} \ldots) \ldots,$$
$$T_2 T_1^{-1} = (a_1)(a_{j_2} a_{j_1} \ldots) \ldots,$$

d'où

$$T_1 T_2^{-1} = T_2 T_1^{-1} = (a_1)(a_{j_1} a_{j_2}) \ldots,$$

ce qui exige $\mathfrak{H}_{a_1} = 2$.

Mais alors évidemment $T_1 = (a_1 a_2) \ldots$ et $T_2 = (a_1 a_2) \ldots$, en sorte que G ne peut appartenir à la classe $N - 1$.

Si, au contraire, $i \neq 1$, on aura $\mathfrak{H}_{a_1} = 3$ et si

$$T_1 = (a_1 a_2 a_{j_1}) \ldots,$$
$$T_2 = (a_1 a_2 a_{j_2}) \ldots,$$
$$T_3 = (a_1 a_2 a_{j_3}) \ldots.$$

comme on a

$$T_1 T_2^{-1} = T_2 T_3^{-1} = T_3 T_1^{-1} = (a_1)(a_{j_1} a_{j_2} a_{j_3}),$$
$$T_1^{-1} T_2 = T_2^{-1} T_3 = T_3^{-1} T_1 = (a_2)(a_{j_1} a_{j_3} a_{j_2}),$$

G ne peut encore appartenir à la classe $N - 1$. C. Q. F. D.

Applications.

I. — Groupes de classe $N - 1$ et de degré $N \leqq 101$.

On voit facilement que ces groupes rentrent dans l'un au moins des cas particuliers que nous venons d'examiner ([1]). On en conclut que des groupes primitifs de degré $N \leqq 101$ et de classe $N - 1$ ne peuvent exister que pour les valeurs de $N = p^m$, p étant un nombre premier, que ces groupes seront de la première catégorie et que les substitutions qui déplacent toutes les lettres sont toutes échangeables entre elles; on sait d'ailleurs qu'il existe effectivement des groupes de classe

([1]) Les groupes de degré 96 s'écartent par un raisonnement direct.

$N = p^m$ et de degré $N - 1$, qui sont linéaires. Nous avons vu que pour $N = p^m$, il n'y en a pas d'autres.

Théorème. — *Les seuls groupes primitifs de classe* $N - 1$ *et de degré* $N \leqq 101$ *sont ceux de degré* $N = p^m$ (*p étant premier*). *Les substitutions de ces groupes qui déplacent toutes les lettres sont toutes échangeables entre elles : ces groupes sont linéaires.*

II. — Groupes de classe $N - 1$ et de degré $N \leqq 1000$ avec $N - 1 = p^\alpha$ (p étant un nombre premier).

L'ordre $\mathcal{G}$ d'un de ces groupes G sera

$$\mathcal{G} = p^\beta (p^\alpha + 1).$$

Si $p = 2$, $N = p^\alpha + 1$ est toujours d'une des formes que nous avons étudiées. Si $p > 2$, G ne serait primitif que si $p = 4h - 1$; si $\alpha = 2\alpha' + 1 > 1$, N est toujours d'une des formes examinées; si α' est nul, $\mathcal{G} = p(p+1)$. On peut donc dire :

Théorème. — *Il n'existe aucun groupe primitif de classe* $N - 1 = p^\alpha$ *et de degré* $N \leqq 1000$ *qui ne soit linéaire et pour lequel on n'ait pas ou* $\alpha = 1$ *avec* $p + 1 = 2^n$, *ou* $p = 2$ *avec* $p^\alpha + 1 = q^m$ (*q premier*).

Complément.

1° Étant donné un groupe G primitif de classe $N - 1$ et de degré $N = \rho f$, f étant un nombre premier quelconque, pour chaque valeur donnée de ρ, f ne peut surpasser $\rho^2 + \rho - 1$.

En effet, d'après le théorème de Sylow,

$$\mathcal{G} = f\nu(af + 1),$$

et $a \geqq 1$, puisque G est primitif. D'après le théorème I,

$$N(N - 1) = \rho f(\rho f - 1) = kf\nu(af + 1),$$
$$k\nu = lf - \rho \qquad \text{avec} \qquad l \geqq 1,$$
$$(\rho f - 1)\rho = (lf - \rho)(af + 1)$$

ou

$$\rho^2 f = alf^2 + (l - a\rho)f,$$
$$\rho^2 = alf + l - a\rho,$$

d'où

$$\rho^2 > a(f-\rho) \geqq f - \rho,$$
$$f < \rho^2 + \rho. \qquad \text{C. Q. F. D.}$$

DEUXIÈME PARTIE.

DES GROUPES TRANSITIFS DE CLASSE N — 2 ET DE DEGRÉ N.

Soit G un groupe transitif de classe N — 2 et de degré N; H_α le groupe de G qui laisse la lettre α immobile, $K_{\alpha\beta}$ le groupe de H_α qui laisse en même temps la lettre β immobile.

Le groupe $K_{\alpha\beta}$ d'ordre $\mathfrak{K}$ est évidemment formé de substitutions régulières, et permute transitivement, $\mathfrak{K}$ à $\mathfrak{K}$, les N — 2 lettres qu'il déplace.

Soient $S_1, S_2, \ldots, S_{\mathfrak{K}}$ les substitutions de $K_{\alpha\beta}$, et T une substitution de H_α de la forme $(\beta\gamma_1\ldots)\ldots$: les substitutions

$$S_1T, \quad S_2T, \quad \ldots, \quad S_{\mathfrak{K}}T$$

qui font partie de H_α remplacent β par γ_1. Aucune autre substitution U de H_α ne remplace β par γ_1 ; sans quoi UT^{-1} ferait partie de $K_{\alpha\beta}$, d'où

$$UT^{-1} = S_i,$$
$$U = S_iT,$$

contrairement à l'hypothèse. Si H_α substitue à β les σ lettres

(7) $$\beta, \quad \gamma_1, \quad \ldots, \quad \gamma_{\sigma-1},$$

on voit qu'on aura dans ce groupe $\mathfrak{K}$ substitutions remplaçant β par γ_i

et que chaque substitution de H_α, à part l'unité, remplacera β par une de ces σ lettres. Si donc $\mathfrak{H}$ est d'ordre de H_α,

$$\mathfrak{H} = \sigma \mathfrak{K}.$$

D'ailleurs, $K_{\alpha\beta}$ laissant β immobile et permutant les $\sigma - 1$ autres lettres (7) transitivement, $\mathfrak{K}$ à $\mathfrak{K}$, on a

$$\sigma = p\mathfrak{K} + 1,$$

$$(8) \qquad \mathfrak{H} = \mathfrak{K}(p\mathfrak{K} + 1),$$

$p = 0$ dans cette formule correspondant au cas où toutes les substitutions de H_α laissent β immobile, ce qui n'a jamais lieu si G est primitif, ou si N est impair.

Les substitutions de H_α qui laissent une des lettres (7) immobile et déplacent toutes les autres, substitutions contenues dans $K_{\alpha\beta}$ et ses transformés par les substitutions de H_α, sont en nombre

$$(\mathfrak{K} - 1)(p\mathfrak{K} + 1) = \frac{\mathfrak{K} - 1}{\mathfrak{K}} \mathfrak{H}.$$

Si parmi les substitutions de H_α il y en avait qui laissaient une lettre δ différente des lettres (7) immobile, cette substitution ne serait pas comprise parmi les $\frac{\mathfrak{K} - 1}{\mathfrak{K}} \mathfrak{H}$ que nous venons de trouver, pas plus que les $\frac{\mathfrak{K}' - 1}{\mathfrak{K}'} \mathfrak{H}$ qu'on en déduirait et qui laisseraient une lettre différente des lettres (7) immobile. On aurait

$$\left(\frac{\mathfrak{K} - 1}{\mathfrak{K}} + \frac{\mathfrak{K}' - 1}{\mathfrak{K}'}\right) \mathfrak{H} < \mathfrak{H},$$

ce qui est absurde. Les substitutions de H_α déplacent donc chacune toutes les lettres autres que α et les lettres (7); la lettre δ différente de α et des lettres (7) est alors permutée transitivement avec $\mathfrak{H}$ autres par les substitutions de H_α et

$$N - 1 = p\mathfrak{K} + 1 + q\mathfrak{H} = (p\mathfrak{K} + 1)(q\mathfrak{K} + 1),$$

où q ne sera nul qui si G est deux fois transitif. D'où :

Théorème I. — *L'ordre* $\mathcal{G}$ *d'un groupe transitif* G *de classe* N — 2 *et de degré* N *est de la forme*

$$\mathcal{G} = \alpha(p\alpha + 1)[(p\alpha + 1)(q\alpha + 1) + 1]$$

avec

$$N = (p\alpha + 1)(q\alpha + 1) + 1,$$

α étant l'ordre du groupe des substitutions de G qui laissent deux lettres immobiles, $\alpha(p\alpha + 1)$ l'ordre du groupe des substitutions de G qui laissent une de ces deux lettres immobiles; on n'a pas $p = 0$ si N impair ou si G primitif; on n'a $q = 0$ que si G est deux fois transitif, et alors

$$\mathcal{G} = \alpha(p\alpha + 1)(p\alpha + 2) \qquad \text{avec} \qquad N = p\alpha + 2.$$

Nous allons maintenant établir, pour les groupes de classe N — 2 et de degré N, un théorème analogue au théorème II de la première partie de ce Chapitre et qui se déduit du théorème général démontré à cette occasion (p. 51).

Théorème II. — *Tout groupe* G′ *d'ordre* $\mathcal{G}' \equiv 0 \pmod{N}$ *contenu dans un groupe* G *transitif de classe* N — 2 *et de degré* N *est transitif entre* N *lettres si* N *est impair. Si* N *est pair, ou bien* G′ *est transitif entre* N *lettres, ou bien il permute ces* N *lettres transitivement entre elles* $\frac{N}{2}$ *à* $\frac{N}{2}$.

Car le plus grand commun diviseur φ de N et de $\frac{\mathcal{G}}{\mathcal{G}'}$ est 1 si N impair; si N pair, φ sera encore égal à 1 si $\frac{\mathcal{G}}{\mathcal{G}'}$ est impair; quand $\frac{\mathcal{G}}{\mathcal{G}'}$ est pair, $\varphi = 2$ et G′ pourra ne pas être transitif. Dans ce dernier cas, les N lettres seront permutées transitivement entre elles, $\frac{N}{2}$ à $\frac{N}{2}$, et G′ sera isomorphe à un groupe transitif de degré $\frac{N}{2}$.

On peut encore montrer qu'il existe, pour les groupes de classe N — 2 et de degré N transitifs, un théorème correspondant au théorème III de la première partie de ce Chapitre.

Nous distinguerons deux cas :

Premier cas. — G est primitif : considérons le groupe H'_α isomorphe à H_α et formé des substitutions opérées par H_α entre les lettres (7). Ce groupe est de classe $N - 2 = (N - 1) - 1$ et de degré $(N - 1)$; il est transitif. Si on lui applique les propriétés trouvées au Chapitre précédent, on voit qu'il ne peut être primitif que si $N - 1 = r^m$ (r premier), pour $N \leqq 101$ et que s'il n'est pas primitif, on aura

$$p\mathfrak{x} + 1 = (n'\mathfrak{x} + 1)(n''\mathfrak{x} + 1) \geqq (\mathfrak{x} + 1)^2$$

avec $n' > 0$, $n'' > 0$,

Deuxième cas. — G n'est pas primitif : si H_α et $K_{\alpha\beta}$ se confondent, c'est-à-dire si $p = 0$, G ne sera pas primitif, et admettra une répartition de ses lettres deux à deux, en sorte que N sera pair. Ce cas mis à part, considérons une répartition quelconque en systèmes de non-primitivité admise par G : le système de cette répartition, qui contient α, a toutes ses lettres permutées exclusivement entre elles par les substitutions de H_α. Le nombre des lettres de ce système sera donc

$$1 + n_1\mathfrak{z} + p\mathfrak{x} + 1 \quad \text{ou} \quad 1 + n'_1\mathfrak{z},$$

suivant que ce système contiendra ou ne contiendra pas les lettres (7).

Supposons d'abord que ce soit $1 + n'_1\mathfrak{z}$; on a

$$(1 + n'_1\mathfrak{z})\psi = N = (p\mathfrak{x} + 1)(q\mathfrak{x} + 1) + 1,$$

et, puisque

$$\mathfrak{z} = \mathfrak{x}(p\mathfrak{x} + 1),$$

$$\psi \equiv 2 (\mathrm{mod}\, \mathfrak{x}) \qquad \text{ou} \qquad \psi = 2 + l\mathfrak{x},$$

d'où

$$1 + n'_1\mathfrak{x}(p\mathfrak{x} + 1) + l\mathfrak{x} + 1 + n'_1\mathfrak{x}(l\mathfrak{x} + 1)(p\mathfrak{x} + 1)$$
$$= (p\mathfrak{x} + 1)(q\mathfrak{x} + 1) + 1,$$

$$l\mathfrak{x} + 1 = \chi(p\mathfrak{x} + 1)$$

et

$$n'_1\mathfrak{x} + n'_1\mathfrak{x}(l\mathfrak{x} + 1) + \chi = q\mathfrak{x} + 1,$$

$$\chi = l_1\mathfrak{x} + 1.$$

Finalement

$$q = l_1 + n'_1(l\mathcal{K} + 2) \geqq p\mathcal{K} + 2,$$

puisque

$$l_1 \geqq 0, \qquad n'_1 \geqq 1, \qquad l \geqq p.$$

Supposons maintenant que ce soit

$$1 + n_1 \mathfrak{Z} + p\mathcal{K} + 1 \quad \text{ou} \quad (n_1\mathcal{K} + 1)(p\mathcal{K} + 1) + 1.$$

Nous opérerons de la même façon; on a

$$[1 + (n_1\mathcal{K} + 1)(p\mathcal{K} + 1)]\psi = \mathrm{N} = (p\mathcal{K} + 1)(q\mathcal{K} + 1) + 1,$$

d'où l'on déduit, quand $\mathcal{K}$ est impair,

$$\psi = 1 + \lambda\mathcal{K},$$
$$\lambda = (p\mathcal{K} + 1)\lambda_1,$$
$$q = \lambda_1 + n_1 + \lambda(n_1\mathcal{K} + 1) \geqq p\mathcal{K} + 2,$$

puisque

$$\lambda_1 \geqq 1, \qquad n_1 \geqq 0, \qquad \lambda \geqq p\mathcal{K} + 1;$$

et quand K est pair :

$$\psi = 1 + \lambda\frac{\mathcal{K}}{2},$$
$$\lambda = (p\mathcal{K} + 1)\lambda_1,$$
$$q = \tfrac{1}{2}\lambda_1 + n_1 + \tfrac{1}{2}\lambda(n_1\mathcal{K} + 1) \geqq \frac{p\mathcal{K} + 2}{2},$$

puisque

$$\lambda_1 \geqq 1, \qquad n_1 \geqq 0, \qquad \lambda \geqq p\mathcal{K} + 1.$$

On obtient ainsi le théorème annoncé.

Théorème III. — *Étant donné le groupe* G *considéré au théorème* I; *si* N *est impair, on a* $q \geqq p\mathcal{K} + 2$; *si* N *est pair, et* $p \neq 0$, *on a* $q \geqq \frac{p\mathcal{K} + 2}{2}$ *ou* $q \geqq p\mathcal{K} + 2$, *suivant que* $\mathcal{K}$ *est pair ou impair;* G *étant supposé, dans tous les cas, non primitif.*

Application. — Si N est impair, et si f est le plus petit nombre premier qui divise $N-2$, $\mathfrak{x} \geqq f$. D'ailleurs

$$\mathcal{G} = \mathfrak{x}(p\mathfrak{x}+1)[(p\mathfrak{x}+1)(q\mathfrak{x}+1)+1]$$

et

$$\mathfrak{x} \geqq f, \qquad p \geqq 1, \qquad q \geqq f+2,$$

d'où

$$N = (p\mathfrak{x}+1)(q\mathfrak{x}+1)+1 \geqq (f+1)^2+1,$$
$$\mathcal{G} \geqq f(f+1)[(f+1)^2+1].$$

En sorte qu'on peut dire :

Parmi les groupes G *transitifs de classe* $N-2$ *et de degré* N, *non primitifs, ceux qui appartiennent à une classe* $\mathfrak{C}$ *impaire ont leur degré*

$$N \geqq (f+1)^2+1$$

et leur ordre

$$\mathcal{G} \geqq f(f+1)[(f+1)^2+1],$$

f étant le plus petit diviseur de $\mathfrak{C}$.

Pour $f=3$,	$N \geqq 65$,	$\mathcal{G} \geqq 12.65$	ou	$\geqq 780$.
Pour $f=5$,	$N \geqq 217$,	$\mathcal{G} \geqq 30.217$	ou	$\geqq 6510$.

....

Les groupes transitifs de classe $N-2$ et de degré N impair, avec $N < 65$, sont donc forcément primitifs.

Le théorème IV de la première Partie de ce Chapitre a aussi son correspondant dans cette deuxième Partie.

Théorème. — *Soit* G *un groupe transitif de classe* $N-2$ *et de degré* N. *Si l'on peut y trouver un groupe* M *ne contenant avec l'unité que des substitutions qui déplacent toutes les lettres, et permutable aux substitutions de* G *qui déplacent toutes les lettres,* G *ne sera pas primitif si* $\mathfrak{M}$ *n'est pas divisible par tous les facteurs pre-*

miers de N. *Il en est de même si* M *est permutable aux substitutions d'un groupe permutable aux substitutions de* G.

La démonstration est semblable à celle que nous avons donnée dans la première Partie. Il n'y a à y supprimer que ce qui est relatif à la distinction en catégories, distinction que nous n'avons pas faite pour les groupes de classe $N - 2$, parce que nous n'en avons trouvé aucune application saillante, mais qu'on pourrait évidemment faire d'une façon analogue.

Examen de quelques valeurs particulières du degré N.

Parmi les groupes transitifs de classe $N - 2$ et de degré N, il y en a qui sont deux fois transitifs, d'autres qui ne le sont qu'une. Nous allons d'abord établir quelques propriétés particulières communes à ces deux séries de groupes, puis nous passerons à l'examen spécial de chacune de ces séries.

I. — $N = 4h + 2$.

On voit facilement que G ne peut être primitif que si $\mathfrak{x}$ est un nombre pair.

II. — $N = \mathfrak{x} + 2$.

Si l'on n'a pas $\mathfrak{g} = \mathfrak{x}(\mathfrak{x} + 2)$, $\mathfrak{x}$ pair, G est trois fois transitif et le groupe de G, qui laisse une lettre H_α immobile, est linéaire, deux fois transitif avec $\mathfrak{x} + 1 = r^m$, r étant un nombre premier.

C'est notamment le cas où $N = f + 2$, f étant un nombre premier > 2 : G ne peut exister que si $f + 1 = 2^m$.

III. — $N = f + 1$.

f étant un nombre premier > 2, G est évidemment deux fois transitif, si $p > 0$.

IV. — $N = 2f + 1$.

f étant un nombre premier > 2,

$$\mathfrak{g} = \mathfrak{x}(p\mathfrak{x} + 1)[(p\mathfrak{x} + 1)(q\mathfrak{x} + 1) + 1]$$

et

$$N = (p\mathfrak{x} + 1)(q\mathfrak{x} + 1) + 1$$

donneraient $p = 0$ et, par suite, N pair, ce qui n'est pas, ou $q = 0$; donc :

Si $N = 2f + 1$, G *est deux fois transitif.*

V. — $N = f^2 + 2$.

f étant un nombre premier > 2,

$$\mathcal{G} = \mathfrak{x}(p\mathfrak{x} + 1)[(p\mathfrak{x} + 1)(q\mathfrak{x} + 1) + 1],$$

et $\mathfrak{x} = f^2$ ou f avec $p > 0$, puisque $N = f^2 + 2$ est impair.

Si l'on avait $\mathfrak{x} = f^2$, G serait 3 fois transitif; H_α serait 2 fois transitif et appartiendrait à la classe $(N - 1) - 1$, son degré étant $N - 1$, ce que nous avons vu impossible.

Si l'on avait $\mathfrak{x} = f$,

$$(pf + 1)(qf + 1) = N - 1 = f^2 + 1.$$

On sait que $p > 0$, puisque $N = f^2 + 2$ est impair; donc

$$q = 0, \qquad p = f,$$
$$\mathcal{G} = f(f^2 + 1)(f^2 + 2),$$

G serait 2 fois transitif; H_α serait alors un groupe transitif de degré $(N - 1)$ et de classe $(N - 1) - 1$, ce que nous savons impossible.

Nous avons supposé $f > 2$; pour $f = 2$ et $N = 6$, on sait, d'après M. Jordan (*Comptes rendus*, 2 octobre 1871), qu'il y a un groupe 3 fois transitif de classe 4 et de degré 6 formé des substitutions linéaires fractionnaires

$$\left| x;\ \frac{ax + \alpha}{bx + \beta} \right| \qquad (\text{mod}\, 5),$$

et un groupe 2 fois transitif de classe 4 et de degré 6, d'ordre moitié moindre, contenu dans le précédent et formé des substitutions pour lesquelles

$$a\beta - b\alpha \equiv z^2 \qquad (\text{mod}\, 5).$$

VI. — $N - 2 = ff'$.

(f et f' étant premiers avec $f < f'$),

$$\mathcal{G} = \mathfrak{x}(p\mathfrak{x} + 1)[(p\mathfrak{x} + 1)(q\mathfrak{x} + 1) + 1].$$

Si $q = 0$ ou si $\mathfrak{x} = ff'$, G ne peut être primitif que s'il est 2 fois transitif (en tout cas G est 2 fois transitif s'il est de degré impair avec $q = 0$ ou $\mathfrak{x} = ff'$).

Si $q > 0$, soit f_1 un des deux facteurs f et f' : $\mathfrak{x} = f_1$. Si, de plus, G est primitif ou N impair, $p \geqq 1$. Dans le cas de $p = 1$, on aura évidemment $f_1 + 1 = 2^m$; f_1 sera, d'ailleurs, égal à f, car

$$(pf_1 + 1)(qf_1 + 1) = (p + q)f_1 + pqf_1^2 + 1 = ff' + 1$$

entraîne

$$f_1 = f \qquad \text{et} \qquad f + 1 = 2^m.$$

Dans le cas de $p > 1$,

$$ff' = (p + q)f_1 + pqf_1^2 = (p + q)f + pqf^2,$$
$$f' = (p + q) + pqf \geqq 2f + 3.$$

On voit ainsi que :

Si G est primitif ou transitif et de degré impair, il faut ou que G soit 2 fois transitif, ou que $f + 1 = 2^m$ ou que $f' \geqq 2f + 3$.

Cette propriété a évidemment lieu pour tous les groupes transitifs G pour lesquels $f > 2$, puisque alors $N = ff' + 2$ est impair.

VII. — $N = 4h + 3$, avec $\mathcal{G} = 4k + 2$,

$$\mathcal{G} = \mathfrak{x}(p\mathfrak{x} + 1)[(q\mathfrak{x} + 1)(p\mathfrak{x} + 1) + 1]$$

montre que $p\mathfrak{x} + 1$ est pair, et puisque $p\mathfrak{x} + 1$ divise $N - 1$,

$$p\mathfrak{x} + 1 = 4h_1 + 2.$$

On sait que G contient un groupe d'ordre $\frac{\mathcal{G}}{2}$ permutable à ses substitutions. Ce groupe G′ est transitif, d'après le théorème II, et de degré N; son ordre sera alors

$$\mathcal{G}' = \frac{\mathcal{G}}{2} = \mathfrak{x}(p'\mathfrak{x}+1)[(q'\mathfrak{x}+1)(p'\mathfrak{x}+1)+1],$$

et, évidemment,

$$p'\mathfrak{x}+1 = 2h_1+1 = \tfrac{1}{2}(p\mathfrak{x}+1),$$
$$p\mathfrak{x}+1 = 2(p'\mathfrak{x}+1),$$

ce qui est absurde.

Il n'existe pas de groupe G *transitif, de classe* N — 2 *et de degré* N = 4*h* + 3, *qui soit d'ordre pair.*

En conséquence, on voit que :

Il n'existe pas de groupe G, *de classe* N — 2 *et de degré* N = 4*h* + 3 *qui soit transitif,* d'après le théorème de la page 98 (¹).

VIII. — $N = f$ (f étant un nombre premier).

L'ordre $\mathcal{G}$ est un diviseur de $(f-2)(f-1)f$ et est $\equiv 0 \pmod{f}$. On sait alors d'après le théorème de Sylow, ou d'après une formule donnée par M. Mathieu (*Journal de Liouville;* 1861), que

$$\mathcal{G} = f\nu(af+1),$$

$f\nu$ étant l'ordre du groupe des substitutions permutables à un groupe d'ordre f de G, et ν étant $\geqq 2$. Alors $\nu(af+1)$ divise $(f-1)(f-2)$, et

$$(f-1)(f-2) = k\nu(af+1),$$

(¹) On en déduit : 1° qu'il n'existe aucun groupe de classe $p^{2\alpha}$ et de degré $p^{2\alpha}+2$ transitif; 2° qu'il n'existe aucun groupe de classe $p^{2\alpha+1}$ et de degré $p^{2\alpha+1}+2$ transitif avec $p = 4h+1$; p étant dans les deux cas un nombre premier impair.

d'où

$$k\nu \equiv 2 \pmod{f}$$

ou

$$k\nu = 2 + lf,$$

$$(f-1)(f-2) = (2+lf)(af+1)$$

et

$$f^2 - 3f = alf^2 + (2a+l)f.$$

Ceci ne peut avoir lieu que pour $l = 0$, puisque $a \geqq 1$, le groupe G étant de classe $f - 2$. Donc

$$(f-1)(f-2) = 2(af+1)$$

et

$$k\nu = 2,$$

ce qui exige $k = 1$, $\nu = 2$, puisque, d'après M. Mathieu (p. 310 du Mémoire précité), $\nu \geqq 2$.

On en conclut que, pour $N = f$, G doit être 3 fois transitif, ce qui ne peut avoir lieu que si $f = 2^m + 1$. Donc :

Les seuls groupes transitifs de classe $N - 2$ *et de degré* N *premier sont des groupes* 3 *fois transitifs; il peut en exister de degré* N *premier si* $N = 2^m + 1$ *et il n'en existe de degré* N *premier qu'à cette condition.*

IX. — $N = 2f$ (f ÉTANT UN NOMBRE PREMIER > 3), G PRIMITIF.

L'ordre $\mathcal{G} = f\nu(af+1)$, d'après le théorème de Sylow, et c'est un diviseur de $(2f-2)(2f-1)2f$. Donc

$$2(2f-1)(2f-2) = k\nu(af+1),$$

$$k\nu = 4 + lf \qquad \text{avec} \qquad l \geqq 0,$$

$$2(2f-1)(2f-2) = (4+lf)(af+1)$$

ou

$$8f^2 - 12f = alf^2 + (4a+l)f$$

ou

$$(8-al)f=(4a+l)+12.$$

Il est évident, puisque $a \geqq 1$, $l \geqq 0$, G étant primitif, que al est < 8. a et l sont donc limités, sauf pour $l=0$ et l'on voit que, sauf pour de petites valeurs de f, cette égalité ne pourra avoir lieu que si $l=0$. On a alors, en général,

$$l=0, \qquad a=2f-3, \qquad k\nu=4.$$

On en conclut d'abord que $\mathcal{G}$ est divisible par $2f-1$, et G 2 fois transitif. De plus $\mathcal{G}$ est un multiple de $\frac{1}{4}(2f-2)(2f-1)2f$. Ceci a lieu même pour les petites valeurs de f, sauf les valeurs 5, 7, 11, 13, 23, 41, comme on le voit directement.

Si l'on suppose en particulier que $2f-2$ soit de la forme $8h+4$ ou $2f=N$ de la forme $8h+6$, si l'on avait $\nu=1$ et, par suite, $\mathcal{G}=\frac{1}{4}(2f-2)(2f-1)2f$, N serait de la forme $4k+2$, et $\mathfrak{X}$ impair : G ne serait pas primitif. Dans ce cas, $\mathcal{G}$ devra donc être multiple de $\frac{1}{2}(2f-2)(2f-1)2f$, et le groupe H_α d'ordre $\mathfrak{H}$ qui laisse la lettre α immobile sera transitif, de degré $2f-1$ et d'ordre multiple de $(2f-1)\frac{2f-2}{2}$; d'après ce qu'on a vu antérieurement (page 56), H_α sera primitif, linéaire et l'on aura

$$2f-1=r^m \qquad (r \text{ étant premier}).$$

Cette dernière égalité a encore lieu pour $2f=8h+2$.

En général, si $N=2f$ *(*f *étant premier), G ne peut être primitif que s'il est 2 fois transitif; les exceptions n'ont lieu que pour les petites valeurs de N ou de* f*. On doit avoir en même temps* $2f-1=r^m$ *(*r *étant premier).*

X. — $N=\rho f$ (f ÉTANT UN NOMBRE PREMIER > 2 ET ρ QUELCONQUE).

En opérant comme précédemment, on trouve :

En général, si $N=\rho f$ *(*f *étant premier), pour une valeur donnée*

de ρ, G *ne peut être primitif que s'il est* 2 *fois transitif; les exceptions n'ont lieu que pour les petites valeurs de* f, *et, par suite, de* N. *On voit même que, quand* ρ *est impair,* G *doit être* 3 *fois transitif et* $\rho f = 2^m + 1$.

En effet, en conservant les mêmes notations que précédemment, on est conduit à l'égalité

$$(9) \qquad (\rho^3 - al)f = 2a\rho + l + 3\rho^2,$$

ρ étant donné et $a \geqq 1$, $l \geqq 0$; puisque G est primitif, pour des valeurs assez grandes de f, on aura

$$al < \rho^3,$$

et, si $l > 0$, a sera limité; l'égalité précédente sera donc impossible pour f assez grand, sauf si $l = 0$.

Mais alors, si

$$\mathcal{G} = f\nu(af+1)$$

et

$$\rho f(\rho f - 1)(\rho f - 2) = kf\nu(af+1),$$
$$k\nu = 2\rho + lf,$$

et, pour $l = 0$,

$$\rho f(\rho f - 1)(\rho f - 2) = 2\rho f(af+1),$$
$$(\rho f - 1)(\rho f - 2) = 2(af+1).$$

Si ρ est pair, $\mathcal{G}$ est multiple de $\frac{1}{2}\rho f(\rho f - 1)(\rho f - 2)$, et, par suite, deux fois transitif; si ρ est impair, $\mathcal{G}$ sera divisible par $(\rho f - 2)$; on aura alors $\mathfrak{X} = \rho f - 2 = \mathrm{N} - 2$ et G sera trois fois transitif; par suite, $\rho f - 1 = 2^m$.

Il est d'ailleurs facile d'établir une limite inférieure des valeurs de f pour lesquelles le théorème est vrai, ρ étant donné.

Ainsi, pour $\rho = 3$, la formule (9) montre que la plus grande valeur de f pour laquelle on puisse avoir $l > 0$ est $f = 107$. Le théorème est donc vrai pour tous les degrés $\mathrm{N} = 3f$ pour lesquels on a $f > 107$.

XI. — $N = 4h$.

Si $\mathfrak{x}$ est pair, G contient évidemment un groupe transitif d'ordre moitié moindre; si, en particulier, G est deux fois transitif, G contiendra un groupe deux fois transitif d'ordre moitié moindre.

Des groupes primitifs de classe $N - 2$ et de degré N qui sont deux fois transitifs.

Soit G un de ces groupes : le groupe H_α qui laisse la lettre α immobile est transitif, de degré $(N - 1)$ et de classe $(N - 1) - 1$. En lui appliquant ce qu'on a vu dans la première partie de ce Chapitre, on trouve les propriétés suivantes :

Théorème. — *Dans tout groupe deux fois transitif de classe* $N - 2$ *et de degré* N *égal à* $p^m + 1$, $pp_1 + 1$, $pp_1^2 + 1$, $p_1p_2p_3 + 1$, *ou* $\leqq 102$, *le groupe transitif* H_α *entre* $N - 1$ *lettres formé des substitutions de* G *qui laissent immobile une lettre quelconque* α *est tel que les substitutions de* H_α *déplaçant* $N - 1$ *lettres forment avec l'unité un groupe transitif permutable aux substitutions de* H_α. H_α *jouit de la même propriété si* G *est trois fois transitif.*

Car les seules exceptions possibles, correspondant aux valeurs de N égales à 37, 41, 57, 79, 89, 97, 101, s'écartent en remarquant :

1° Que 79 est de la forme $4h + 3$;

2° Que 37, 41, 89, 97, 101 sont des nombres premiers qui ne sont pas de la forme $2^m + 1$, comme d'ailleurs le nombre précédent;

3° Que, si $N = 57$, $\mathcal{G} = \mathfrak{x} \times 56 \times 57$, $\mathfrak{x}$ étant égal à 5 ou 11. On sait d'ailleurs que H_α n'est pas primitif, en sorte que

$$56 = (n'\mathfrak{x} + 1)(n''\mathfrak{x} + 1) \qquad \text{avec} \qquad n' \geqq 1, \qquad n'' \geqq 1,$$

ce qui n'a pas lieu.

Examen du cas particulier où $N \leqq 102$.

Nous allons chercher quelles sont les valeurs de $N \leqq 102$ pour lesquelles on a des groupes de classe $N-2$ et de degré N au moins deux fois transitifs.

Si r est un nombre premier, on en a pour toutes les valeurs de $N = r^m + 1$. Je dis qu'on n'en a pas d'autres.

Pour éliminer successivement toutes les valeurs de N qui ne sont pas de cette forme, nous allons appliquer les résultats précédemment obtenus.

Les nombres

$7 = 5 + 2$	avec	$7 - 1 = 6 \neq 2^m$
$13 = 11 + 2$		$13 - 1 = 12 \neq 2^m$
$15 = 13 + 2$		$15 - 1 = 14 \neq 2^m$
$19 = 17 + 2$		$19 - 1 = 18 \neq 2^m$
$21 = 19 + 2$		$21 - 1 = 20 \neq 2^m$
$25 = 23 + 2$		$25 - 1 = 24 \neq 2^m$
$31 = 29 + 2$		$31 - 1 = 30 \neq 2^m$
$39 = 37 + 2$		$39 - 1 = 38 \neq 2^m$
$43 = 41 + 2$		$43 - 1 = 42 \neq 2^m$
$45 = 43 + 2$		$45 - 1 = 44 \neq 2^m$
$49 = 47 + 2$		$49 - 1 = 48 \neq 2^m$
$55 = 53 + 2$		$55 - 1 = 54 \neq 2^m$
$61 = 59 + 2$		$61 - 1 = 60 \neq 2^m$
$63 = 61 + 2$		$63 - 1 = 62 \neq 2^m$
$69 = 67 + 2$		$69 - 1 = 68 \neq 2^m$
$73 = 71 + 2$		$73 - 1 = 72 \neq 2^m$
$75 = 73 + 2$		$75 - 1 = 74 \neq 2^m$
$81 = 79 + 2$		$81 - 1 = 80 \neq 2^m$
$85 = 83 + 2$		$85 - 1 = 84 \neq 2^m$
$91 = 89 + 2$		$91 - 1 = 90 \neq 2^m$

sont tous de la forme $f + 2$ avec $f + 1 \neq 2^m$. Ils doivent donc être tous écartés.

Les nombres

$$11 = 9 + 2 = 3^2 + 2$$
$$27 = 25 + 2 = 5^2 + 2$$
$$51 = 49 + 2 = 7^2 + 2$$

sont de la forme $f^2 + 2$, f étant premier, et doivent être écartés.

Les nombres

$$23 = 20 + 3 = 4 \times 5 + 3$$
$$35 = 32 + 3 = 4 \times 8 + 3$$
$$47 = 44 + 3 = 4 \times 11 + 3$$
$$59 = 56 + 3 = 4 \times 14 + 3$$
$$67 = 64 + 3 = 4 \times 16 + 3$$
$$71 = 68 + 3 = 4 \times 17 + 3$$
$$79 = 76 + 3 = 4 \times 19 + 3$$
$$83 = 80 + 3 = 4 \times 20 + 3$$
$$87 = 84 + 3 = 4 \times 21 + 3$$
$$95 = 92 + 3 = 4 \times 23 + 3$$
$$99 = 96 + 3 = 4 \times 24 + 3$$

sont tous de la forme $4h + 3$ et doivent être écartés.

Les nombres

29	avec	$29 - 1 = 28 \neq 2^m$
37		$37 - 1 = 36 \neq 2^m$
41		$41 - 1 = 40 \neq 2^m$
97		$97 - 1 = 96 \neq 2^m$
53		$53 - 1 = 52 \neq 2^m$
89		$89 - 1 = 88 \neq 2^m$
101		$101 - 1 = 100 \neq 2^m$

sont premiers et $\neq 2^m + 1$: ils doivent être écartés.

Le nombre 57, pour lequel $\mathcal{G}$ est égal à $\mathfrak{x} \times 56 \times 57$, et pour lequel

H_α n'est pas primitif, est tel que l'ordre de H_α ne peut satisfaire au théorème III de la première partie de ce Chapitre : il doit être écarté.

Il ne nous reste à considérer spécialement que les valeurs de N égales à

$$16,\ 22,\ 34,\ 36,\ 40,\ 46,\ 52,\ 56,\ 58,\ 64,\ 66,$$
$$70,\ 76,\ 77,\ 78,\ 86,\ 88,\ 92,\ 93,\ 94,\ 96,\ 100$$

que nous allons examiner successivement.

$$N = 93.$$

La formule $\mathcal{G} = \mathcal{X}(p\mathcal{X}+1)(p\mathcal{X}+2)$ conduit à une absurdité.

$$N = 77.$$

D'après la formule

$$\mathcal{G} = \mathcal{X}(p\mathcal{X}+1)(p\mathcal{X}+2)$$

avec

$$N = p\mathcal{X}+2 = 77,$$

et en remarquant que H_α d'ordre $\mathcal{X}(p\mathcal{X}+1)$ ne peut être primitif, et que, par suite,

$$p\mathcal{X}+1 = (n'\mathcal{X}+1)(n''\mathcal{X}+1),$$

on voit que

$$\mathcal{X} = 3 \qquad \text{et} \qquad \mathcal{G} = 3 \times 76 \times 77.$$

Les substitutions d'ordre 7 et 11 déplacent toutes les lettres; le nombre des substitutions d'ordre 7 est dès lors multiple de 6 et de 3×76 et cette condition montre, en appliquant le théorème de Sylow, que G ne peut renfermer que 33×38 groupes d'ordre 7, soit $3 \times 76 \times 33$ substitutions d'ordre 7, ce qu'on voit facilement être absurde en comptant le nombre de substitutions de classes 75 et 76. La valeur $N = 77$ doit donc être écartée, et il ne reste plus à examiner que des valeurs paires de N.

En général, pour ces valeurs paires de N, le groupe H_α ne peut être primitif, d'après ce qu'on a vu dans la première partie de ce Chapitre : on peut dès lors appliquer aux groupes H_α correspondants le théo-

rème III de cette première partie, on voit que, pour ces valeurs de N, on ne peut avoir pour $\mathcal{G}$ que les valeurs

2.15.16	2.55.56	2.85.86 ou 4.85.86
2.21.22	2.57.58	2.87.88
2.33.34	2.63.64	2.91.92 ou 3.91.92 ou 6.91.92
2.35.36	2.65.66 ou 4.65.66	2.93.94
2.39.40	2.69.70	2.95.96
2.45.46 ou 4.45.46	2.75.76	2.99.100
2.51.52	2.77.78	

$N = 2f$, f ÉTANT UN NOMBRE PREMIER.

$\varkappa$ est égal à 2^i avec $i = 1$ ou 2, et pour $i = 2$, $f = 4h + 3$, G contient un nombre de substitutions d'ordre f qui est multiple de $f - 1$ et de $2^i(2f - 1)$, par suite, de $(f - 1)(2f - 1)$ pour $i = 1$ et de $2(f - 1)(2f - 1)$ pour $i = 2$.

D'après le théorème de Sylow

$$\mathcal{G} = f\nu(af + 1) = 2^i(2f - 1)2f,$$

ce qui donne, pour $i = 1$,

$$af + 1 = \psi \times (2f - 1), \qquad \psi \text{ divisant } 4,$$

et pour $i = 2$,

$$af + 1 = \psi \times 2 \times (2f - 1), \qquad \psi \text{ divisant } 4.$$

La première condition donne

$$-\psi \equiv 1 \qquad (\text{mod } f),$$

et la deuxième

$$-2\psi \equiv 1 \qquad (\text{mod } f),$$

ce qui ne peut avoir lieu, puisque les valeurs de f considérées sont > 9. On écarte donc ainsi les valeurs de N égales à 22, 34, 46, 58, 86 et 94.

$$N = 32, 56, 76, 78, 88, \textit{ou } 92.$$

Ces nombres s'écartent par un raisonnement tout à fait analogue au précédent.

$$N = 4h.$$

Pour les valeurs de N de cette forme, $\varkappa = 2$, et d'après ce qu'on a vu antérieurement, G renferme un groupe G′ transitif d'ordre moitié moindre, lequel est évidemment deux fois transitif, de classe $N - 1$ et de degré N : donc $N = 2^m$ et les valeurs de N égales à 36, 40, 96, 100 se trouvent ainsi écartées.

Mais il reste les valeurs 16 et 64 pour lesquelles les groupes G et G′ sont évidemment linéaires (mod 2). Le groupe G contiendra alors une substitution linéaire (mod 2) laissant immobiles deux des N lettres seulement, le nombre d'indices des substitutions de G étant d'ailleurs égal à m si $N = 2^m$. Mais si l'on suppose cette substitution linéaire ramenée à sa forme canonique, il est facile de voir qu'elle sera de la forme

$$\left| \begin{array}{ll} x_1; & x_1 \\ x_2; & x_1 + x_2 \\ x_3; & x_3 \\ x_4; & x_3 + h_4 x_4 \\ \ldots; & \ldots\ldots\ldots\ldots \end{array} \right| \pmod{2},$$

les coefficients $h_4, h_6, \ldots$ pouvant être congrus à 0 ou 1 (mod 2). La transformation d'indices est, d'ailleurs, évidemment réelle, et cette substitution laisse forcément au moins $2^{\frac{m}{2}}$ lettres immobiles.

On en conclut qu'il peut exister effectivement des groupes 2 fois transitifs de degrés 16 et 64 et d'ordres respectifs $2 \times 15 \times 16$ et $2 \times 63 \times 64$, mais qu'ils appartiennent respectivement à des classes paires inférieures à 14 et 62.

$$N = 70.$$

$\mathfrak{g} = 2 \times 69 \times 70$. Le nombre des substitutions d'ordre 7, lesquelles déplacent toutes les lettres, est multiple de 6×23 et le nombre des

groupes d'ordre 7 contenus dans G est multiple de 23 : si ce nombre est $\psi \times 23$, on a

$$\psi \times 23 \equiv 1 \pmod 7,$$

ψ divisant $\frac{\mathcal{G}}{23 \times 7} = 60$; ψ ne peut avoir que les valeurs 4 ou 60. $\psi = 60$ donnerait $60 \times 23 \times 6$ substitutions d'ordre 7, ce qui ne peut avoir lieu à cause du nombre de substitutions de classe 69 et 68 que doit renfermer G : on a donc $\psi = 4$,

$$\mathcal{G} = 7 \times 15 \times (4 \times 23).$$

La quantité ν de la formule de Sylow correspondant à un groupe d'ordre 7 de G est égale à 15, en sorte que G renferme un groupe L d'ordre 7×15 qui contient un groupe d'ordre 7 permutable à ses substitutions. L renferme un groupe L′ d'ordre 7×5 formé de substitutions échangeables, et, par suite, des puissances d'une substitution d'ordre 35, déplaçant toutes les lettres. Si deux groupes d'ordre 35 contenus dans G, L′ et L″ avaient en commun une substitution d'ordre 7 ou 5, le groupe dérivé (L′, L″), contenant une substitution d'ordre 7 ou 5 échangeable à toutes ses substitutions, serait d'ordre $\chi \times 35$, avec $\chi = 2$ ou 4 et, d'après le théorème de Sylow, ce groupe ne renfermerait qu'une substitution d'ordre 7 et ses puissances et qu'une d'ordre 5 et ses puissances; par suite, ce groupe ne renfermerait qu'un groupe d'ordre 35, contrairement à l'hypothèse. L′ et L″ ne peuvent donc avoir en commun que la substitution 1. Il en résulte qu'à chaque groupe d'ordre 7 correspondra dans G un groupe d'ordre 35, de même qu'à chaque groupe d'ordre 5. Le nombre des groupes d'ordre 35, par suite, celui des groupes d'ordre 5, sera donc 4×23.

Mais le nombre des groupes d'ordre 5 contenu dans G ne peut être 4×23, puisque

$$4 \times 23 \equiv 2 \pmod 5.$$

Il n'existe donc aucun groupe de degré 70 et de classe 68 qui soit 2 fois transitif.

$$N = 66.$$

En raisonnant comme tout à l'heure, on voit pour les deux valeurs

de $\mathcal{G}$ égales à $2 \times 65 \times 66$ ou $4 \times 65 \times 66$ que G ne peut exister que s'il renferme 78 substitutions d'ordre 11.

Si $\mathcal{G} = 2 \times 65 \times 66 = 78 \times 11 \times 10$, d'après le théorème de Sylow, G renferme un groupe L d'ordre 110 contenant un groupe d'ordre 11 permutable à ses substitutions. Une substitution d'ordre 11 ne peut évidemment être échangeable à une d'ordre 2 ou 5 et L renfermera alors un groupe M d'ordre 10, d'après le théorème de Sylow. Ce groupe ne peut être formé de substitutions échangeables, parce que dans G une substitution d'ordre 2 et une d'ordre 5 ne peuvent être échangeables : M renferme donc une substitution d'ordre 2 permutable à un groupe d'ordre 5. D'autre part, le groupe L est isomorphe à un groupe transitif dont l'ordre égale le degré 110, qui renferme un groupe maximum d'ordre 10. On déduit alors de ce groupe transitif par le théorème IV du premier Chapitre un groupe de degré 11 et d'ordre 11×10 contenant une substitution d'ordre 10. On est donc conduit à une contradiction et l'on ne peut avoir $\mathcal{G} = 2 \times 65 \times 66$.

Si $\mathcal{G} = 4 \times 65 \times 66 = 78 \times 11 \times 20$, le même raisonnement simplifié donne un groupe de degré 11 et d'ordre 11×20 contenant un groupe d'ordre 11 permutable à ses substitutions, ce qui est absurde, ou un groupe de degré 11 et d'ordre $< 11 \times 20$ à la condition qu'on ait une substitution d'ordre 2 ou 5 échangeable à une d'ordre 11, ce qui est absurde : on ne peut donc avoir $\mathcal{G} = 4 \times 65 \times 66$.

Il n'y a donc aucun groupe 2 fois transitif de classe 64 et de degré 66.

Nous avons ainsi écarté toutes les valeurs de N qui ne sont pas de la forme $r^m + 1$.

THÉORÈME. — *Les valeurs de* $N \leqq 102$ *pour lesquelles on peut avoir des groupes* G, 2 *ou* 3 *fois transitifs, de classe* $N - 2$ *et de degré* N, *sont de la forme* $r^m + 1$, *r étant premier* [1] :

1° *Valeurs de* N *pour lesquelles on peut avoir à la fois des groupes* 2 *et* 3 *fois transitifs de classe* $N - 2$ *et de degré* N,

6, 8, 10, 12, 14, 18, 20, 24, 26, 28, 30, 32, 38, 42, 44, 48, 50, 54, 60, 62, 65, 68, 72, 74, 80, 82, 84, 90, 98, 102.

(1) On peut encore montrer, par des procédés analogues, que le groupe H_α des substitutions de G qui laissent une lettre α immobile est primitif pour $N \leqq 102$.

2° *Valeurs de* N *pour lesquelles on ne peut avoir que des groupes* 3 *fois transitifs de classe* $N - 2$ *et de degré* N,

$$4,\ 5,\ 9,\ 17,\ 33.$$

Des groupes primitifs de classe N — 2 et de degré N qui ne sont qu'une fois transitif.

D'après ce qu'on a vu, on ne peut en avoir aucun pour

$N = f + 2$,
$N = f + 1$,
$N = 2f + 1$,
$N = f^2 + 2$ avec $f > 2$,
$N = ff' + 2$ avec $f + 1 \neq 2^m$ et $f' < 2f + 3$,
$N = 4h + 3$ avec g pair,
$N = f$,
$N = 2f$, f étant différent de 5, 7, 11, 13, 23 ou 41,
$N = \rho f$, ρ étant donné et f étant suffisamment grand. f et f' sont des nombres premiers.

On en conclut que le seul groupe de classe $N - 2$ et de degré $N \leqq 102$ primitif, 1 fois transitif, est de degré 10.

En effet, les nombres

$4 = 2 + 2$	$45 = 43 + 2$
$5 = 3 + 2$	$49 = 47 + 2$
$7 = 5 + 2$	$55 = 53 + 2$
$9 = 7 + 2$	$61 = 59 + 2$
$13 = 11 + 2$	$63 = 61 + 2$
$15 = 13 + 2$	$69 = 67 + 2$
$19 = 17 + 2$	$73 = 71 + 2$
$21 = 19 + 2$	$75 = 73 + 2$
$25 = 23 + 2$	$81 = 79 + 2$

$31 = 29 + 2$	$85 = 83 + 2$
$33 = 31 + 2$	$91 = 89 + 2$
$39 = 37 + 2$	$99 = 97 + 2$
$43 = 41 + 2$	

sont tous de la forme $f + 2$ et doivent être écartés.

Les nombres

$6 = 5 + 1$	$44 = 43 + 1$
$8 = 7 + 1$	$48 = 47 + 1$
$12 = 11 + 1$	$54 = 53 + 1$
$14 = 13 + 1$	$60 = 59 + 1$
$18 = 17 + 1$	$62 = 61 + 1$
$20 = 19 + 1$	$68 = 67 + 1$
$24 = 23 + 1$	$72 = 71 + 1$
$30 = 29 + 1$	$74 = 73 + 1$
$32 = 31 + 1$	$80 = 79 + 1$
$38 = 37 + 1$	$84 = 83 + 1$
$42 = 41 + 1$	$90 = 89 + 1$
$98 = 97 + 1$	$102 = 101 + 1$

sont de la forme $f + 1$ et doivent être écartés.

Les nombres

11, 17, 23, 29, 37, 41, 47, 53, 59, 67, 71, 79, 83, 89, 97, 101

sont tous premiers et doivent être écartés.

Les nombres

$$27 = 2 \times 13 + 1$$
$$35 = 2 \times 17 + 1$$
$$87 = 2 \times 43 + 1$$
$$95 = 2 \times 47 + 1$$

sont tous de la forme $2f + 1$ et doivent être écartés.

Les nombres

$$34 = 2 \times 17$$
$$58 = 2 \times 29$$
$$86 = 2 \times 43$$
$$94 = 2 \times 47$$

sont de la forme $2f$ et ne rentrent pas dans les cas d'exceptions possibles : ils doivent être écartés.

Le nombre

$$51 = 49 + 2 = 7^2 + 2$$

est de la forme $f^2 + 2$ avec $f > 2$ et doit être écarté.

Le nombre

$$57 = 55 + 2 = 5 \times 11 + 2 \quad \text{avec} \quad 5 + 1 \neq 2^m \quad \text{et} \quad 11 < 2 \times 5 + 3$$

est de la forme $ff' + 2$,

$$f' < 2f + 3 :$$

il doit être écarté.

Il ne nous reste alors à examiner que les valeurs impaires de N :

$$65, \ 77, \ 93,$$

et les valeurs paires :

$$10, \ 16, \ 22, \ 26, \ 28, \ 36, \ 40, \ 46, \ 50, \ 52, \ 56,$$
$$64, \ 66, \ 70, \ 76, \ 78, \ 82, \ 88, \ 92, \ 96, \ 100.$$

Pour tous ces groupes, la quantité q du théorème I est > 0.

N *impair*. — Les seules valeurs de $\mathcal{G}$ admissibles, d'après le théorème I, sont :

$$3 \times 4 \times 65, \quad 3 \times 16 \times 65, \quad 7 \times 8 \times 65,$$
$$3 \times 4 \times 77, \quad 3 \times 19 \times 77,$$

la valeur $N = 93$ ne pouvant satisfaire au théorème I.

$N = 65.$

1° $\mathcal{G} = 3 \times 4 \times 65$. — Le théorème de Sylow montre que ce groupe ne contient qu'un groupe d'ordre 13 : il ne serait donc pas primitif.

2° $\mathcal{G} = 7 \times 8 \times 65$. — Le théorème de Sylow montre que, étant donné un groupe d'ordre 5, les substitutions qui lui sont permutables dans G forment un groupe d'ordre 65, et que, étant donné un groupe d'ordre 13, les substitutions qui lui sont permutables forment un groupe d'ordre $260 = 13 \times 5 \times 4$. Les substitutions de ce groupe d'ordre 260 permutables à un groupe d'ordre 5 contenu dedans forment un groupe d'ordre 65 ou d'ordre 5 : d'après Sylow, ce ne peut être d'ordre 5 : c'est donc d'ordre 65. Ce groupe d'ordre 260 a alors toutes ses substitutions permutables à un groupe d'ordre 5, et un groupe d'ordre 5 de G serait permutable aux substitutions d'un groupe de G d'ordre multiple de 260. On est ainsi conduit à une contradiction.

3° $\mathcal{G} = 3 \times 16 \times 65$. — Le théorème de Sylow montre que le nombre des groupes d'ordre 13 ne peut être que 40,

$$\mathcal{G} = 6 \times 13 \times 40$$

et les substitutions de G permutables à ce groupe d'ordre 13 forment un groupe d'ordre 78, que nous désignons par K.

K et G ne renferment aucune substitution d'ordre 2 ou 3 échangeable à une d'ordre 13. Si alors on considère le groupe transitif dont l'ordre égale le degré 78 isomorphe à K, ce groupe renferme un groupe maximum d'ordre 6 et, d'après le théorème IV du premier Chapitre, on en déduit un groupe de degré 13 et d'ordre 78 renfermant une substitution d'ordre 6 contenant une substitution d'ordre 2 et une d'ordre 3 échangeable, ce qui n'a pas lieu pour G.

On voit ainsi que, en tout cas, la valeur $N = 65$ doit être écarté.

$N = 77.$

1° $\mathcal{G} = 3 \times 4 \times 77$. — D'après le théorème de Sylow, le nombre des groupes d'ordre 11 contenu dans G est de 12 : $\mathcal{G} = 7 \times 11 \times 12$.

G contient donc un groupe d'ordre 77 formé de substitutions échangeables.

Le nombre des groupes d'ordre 7 contenus dans G est alors un diviseur de 12 et est $\equiv 1 \pmod 7$, d'après le théorème de Sylow; il n'y en aurait donc qu'un et G ne serait pas primitif.

2° $\mathcal{G} = 3 \times 19 \times 77$. — Le théorème de Sylow montre que G ne pourrait renfermer qu'un groupe d'ordre 11; G ne serait donc pas primitif.

En résumé, le nombre $N = 77$ doit être écarté.

N *pair*. — On limite encore par l'application du théorème I le nombre de valeurs de $\mathcal{G}$ admissibles.

$N = 10$. — La seule valeur de $\mathcal{G}$ admissible est

$$\mathcal{G} = 10 \times 3 \times 2.$$

On sait qu'il existe effectivement un groupe primitif de degré 10, de classe 8, une seule fois transitif (JORDAN, *Comptes rendus*, 23 décembre 1872).

$N = 4h$. — Le théorème I montre que les seules valeurs possibles de $\mathcal{G}$ sont :

2.3.16 ou 2. 5.16	2.3. 64 ou 2.9. 64 ou 2.21. 64 ou 2. 7. 64
2.3.28 ou 2. 9.28	2.3. 76 ou 2.5. 76 ou 2.15. 76 ou 2.25. 76
2.5.36 ou 2. 7.36	2.3. 88 ou 2.29. 88
2.3.40 ou 2.13.40	2.7. 92 ou 2.13. 92
2.3.52 ou 2.17.52	3.7. 92 ou 3.13. 92
2.5.56 ou 2.11.56	6.7. 92 ou 6.17. 92
2.5.96 ou 2.19.96	2.3.100 ou 2.9.100 ou 2.11.100 ou 2.33.100

Tous ces groupes, sauf deux de degré 92, contiennent, d'après ce qu'on a dit antérieurement, un groupe G′ d'ordre $\mathcal{G}' = \frac{\mathcal{G}}{2}$. Si l'on peut trouver dans G′, qui est permutable aux substitutions de G, un groupe M permutable aux substitutions de G′ et ne contenant, avec l'unité, que des substitutions qui déplacent toutes les lettres; si, de plus, $\mathfrak{M}$ n'est pas divisible par tous les facteurs premiers de N, G ne pourra être primitif.

C'est en particulier le cas quand $\mathfrak{x} = 2$ et que $N = 4f$, f étant pre-

mier et > 2, G′ étant alors un groupe transitif de classe $N - 1$ et de degré N, d'après ce qu'on a vu dans la première partie de ce Chapitre. Les valeurs de N égales à 28, 52, 76 doivent ainsi être écartées, ainsi que les valeurs de $\mathcal{G} = 2 \times 7 \times 92$ ou $\mathcal{G} = 2 \times 13 \times 92$, correspondant à $N = 92$.

En général, quand $\mathfrak{X} = 2$, G′ renferme un groupe K transitif dont l'ordre égale le degré N permutable aux substitutions de G′. On voit facilement, soit à l'aide du théorème de Sylow, soit à l'aide des raisonnements faits dans la première partie de ce Chapitre pour $N = 36$, qu'on a toujours dans K un groupe M d'ordre $\mathfrak{M}$ permutable aux substitutions de G′, $\mathfrak{M}$ n'étant pas divisible par tous les diviseurs premiers de N. On écarte ainsi les valeurs de N égales à 36, 40, 56, 88. Mais ce raisonnement n'est pas applicable aux valeurs de $N = 2^m$, c'est-à-dire aux valeurs de N égales à 16 ou 64.

On voit facilement, par un raisonnement analogue à celui de la page 54, que, si G est primitif pour ces valeurs de N, il doit être linéaire : nous avons, d'ailleurs, vu que les substitutions linéaires (mod 2) à quatre et six indices, qui laissent deux lettres immobiles, doivent en laisser en même temps d'autres, en sorte que les valeurs de N égales à 16 et 64 doivent aussi être écartées.

Les valeurs de $\mathcal{G}$, égales à $3 \times 13 \times 92$ ou $3 \times 7 \times 92$, s'écartent par le théorème de Sylow qui montre que les groupes correspondants ne contiendraient qu'un groupe d'ordre 23.

Enfin, pour les valeurs de $\mathcal{G}$, égales à $6 \times 13 \times 92$ ou $6 \times 7 \times 92$, les groupes G correspondants contiennent évidemment un groupe G′ d'ordre $\frac{\mathcal{G}}{2} = \mathcal{G}'$ permutable aux substitutions de G. Le théorème III montre facilement que G′ doit être primitif; mais nous venons de voir qu'il n'y a pas de groupes primitifs d'ordre $\mathcal{G}'$. La valeur de N égale à 92 doit donc, en résumé, être écartée.

N *égal à* 22, 26, 46, 82.

Les seuls groupes qui puissent exister seraient d'ordre

$$2 \times 3 \times 22 \quad \text{ou} \quad 2 \times 7 \times 22$$
$$2 \times 5 \times 26 \quad \text{ou} \quad 4 \times 5 \times 26$$
$$2 \times 3 \times 46, \quad 2 \times 9 \times 46, \quad 2 \times 5 \times 46, \quad 2 \times 15 \times 46, \quad 4 \times 9 \times 46$$

ou

$$4 \times 5 \times 46, \quad 2 \times 3 \times 82, \quad 2 \times 9 \times 82$$
$$2 \times 27 \times 82, \quad 4 \times 9 \times 82, \quad 8 \times 9 \times 82$$

Pour la plupart d'entre eux, le théorème e Sylow, joint ou non à cette remarque que, si $\mathcal{G} = \mathfrak{x}(p\mathfrak{x}+1)\mathrm{N}$, G contient $p\mathfrak{x}\mathrm{N}$ substitutions de classe $\mathrm{N}-1$ et $\mathrm{N}(p\mathfrak{x}+1)\frac{\mathfrak{x}-1}{2}$ substitutions de $\mathrm{N}-2$, montre que G ne peut être primitif. Pour le groupe G d'ordre $\mathcal{G} = 4 \times 9 \times 46$, on remarque que, d'après le théorème de Sylow, on aurait dans G une substitution d'ordre 3 et une d'ordre 23 échangeable, ce qui est absurde : les valeurs de N égales à 22, 26, 46, 82 doivent donc être écartées.

$$\mathrm{N} = 50.$$

N étant de la forme $4h+2$, $\mathfrak{x}$ doit être pair, et $\mathcal{G}$ est égal à $2 \times 7 \times 50$ ou $6 \times 7 \times 50$.

Pour $\mathcal{G} = 2 \times 7 \times 50$, G ne renfermerait qu'un groupe d'ordre 25, d'après le théorème de Sylow, et ne serait pas primitif.

Pour $\mathcal{G} = 6 \times 7 \times 50$, deux groupes d'ordre 25 n'ont évidemment d'autre substitution commune que l'unité, sans quoi dans le groupe dérivé on aurait une substitution d'ordre 5, échangeable à une substitution laissant une ou deux lettres immobiles, ce qui est absurde, ou une substitution d'ordre 2 déplaçant toutes les lettres et ne faisant pas partie du groupe alterné de 50 éléments, auquel cas G ne serait pas primitif. Le nombre des substitutions d'ordre 5 ou 25 est alors multiple de 24 et de 42, par suite de 24×7; le nombre des groupes d'ordre 25 est donc multiple de 7, et, d'après le théorème de Sylow, il ne peut être égal qu'à 21. En comptant alors les substitutions d'ordre 5 et 25 et celles de classe 49 et 48, on voit qu'il y a dans G des substitutions de classe 50 qui ne sont pas d'ordre 5, ou 25, et sont, par suite, d'ordre pair. Elles ne sont pas régulières, sans quoi on aurait dans G une substitution d'ordre 2 ne faisant pas partie du groupe alterné de 50 éléments et G ne serait pas primitif. G étant de classe 48, elles renfermeront un cycle d'ordre 2 et d'autres cycles comptant tous le même nombre de lettres. Ces substitutions S, S', ..., élevées à la

puissance 2, donnent une substitution d'ordre diviseur de 6. S, par exemple, sera d'ordre 2, 4, 6 ou 12. Mais alors les formes respectives de S montrent que S ne fait pas partie du groupe alterné de 50 éléments, et que G n'est pas primitif.

La valeur $N = 50$ doit donc être écartée.

$$N = 66.$$

$\mathcal{G}$ peut être égal à

$$2 \times 5 \times 66, \quad 4 \times 5 \times 66, \quad 2 \times 13 \times 66 \quad \text{ou} \quad 4 \times 13 \times 66.$$

Pour $\mathcal{G} = 2 \times 5 \times 66$. — D'après le théorème de Sylow, si G est primitif, G renferme douze groupes d'ordre 11 et les substitutions permutables à un groupe d'ordre 11 forment un groupe d'ordre 55. Par un procédé déjà appliqué plusieurs fois, on en conclut que G est isomorphe à un groupe deux fois transitif G_1 d'ordre $12 \times 11 \times 5$ et de degré 12. On voit facilement que, si G est primitif, deux groupes d'ordre 4 de G_1 ne peuvent avoir d'autres substitutions communes que l'unité, et que le nombre des groupes d'ordre 4 ou 3 de G_1 doit être égal à 55, en sorte que G_1, par suite G, renferme un groupe d'ordre 12 formé de substitutions échangeables; G renferme donc une substitution d'ordre 6, laquelle ne peut être contenue dans le groupe alterné de 66 éléments. G ne serait donc pas primitif.

Pour $\mathcal{G} = 4 \times 5 \times 66$, on voit de même que G est isomorphe à un groupe G_1 de degré 12 et d'ordre $12 \times 11 \times 10$ qui serait trois fois transitif. G_1 renfermerait une substitution d'ordre 10, et il en serait de même pour G, ce qui est absurde.

Pour $\mathcal{G} = 66 \times 13 \times 2$, le nombre des groupes d'ordre 11 contenus dans G est multiple de 13 : il devrait être égal à 78, et l'on voit, en comptant le nombre des substitutions de classe 65 et 64 contenues dans G que cela n'est pas possible. G ne peut donc être primitif.

Pour $\mathcal{G} = 66 \times 13 \times 4$, on voit encore, d'après le théorème de Sylow, que le nombre des groupes d'ordre 13 est de 78. $\mathcal{G} = 78 \times 11 \times 4$ et, d'après le même théorème, G renfermerait un groupe d'ordre 44 renfermant un groupe unique d'ordre 11 permutable à ses substitutions. On voit facilement que ce groupe d'ordre 44 est isomorphe à

un groupe de degré 11 lequel devra évidemment être d'ordre 11×2 ou 11, en sorte que G renfermerait une substitution d'ordre 11 et une d'ordre 2 échangeables. Ceci ne peut avoir lieu que si cette substitution d'ordre 2 déplace toutes les lettres de G, et, par suite, ne fait pas partie du groupe alterné. G ne serait donc pas primitif.

En résumé, la valeur $N = 66$ doit être écartée.

$N = 70.$

$\mathcal{G}$ est égal à $70 \times 3 \times 2$ ou à $70 \times 23 \times 2$.

Si $\mathcal{G} = 70 \times 3 \times 2$, G renfermera, d'après Sylow, quinze groupes d'ordre 7, par suite, un groupe unique 7×4 renfermant un groupe unique d'ordre 7. On voit facilement que ceci ne peut avoirlieu que si G renferme une substitution d'ordre 7 et une d'ordre 2 échangeables, ce qui ne peut avoir lieu si G est primitif.

Si $\mathcal{G} = 70 \times 23 \times 2$, le nombre des groupes d'ordre 7 ou 5 de G est multiple de 23 et le théorème de Sylow montre que G renferme un groupe d'ordre 35 formé de substitutions échangeables, le groupe des substitutions de G permutables à un groupe d'ordre 7 devant simultanément être égal à 35 et $\geqq 70$, ou un groupe d'ordre 5×4, en sorte que G renfermerait plus de substitutions que ne le comporte son ordre, comme on le voit en additionnant le nombre des substitutions d'ordre 5 et 7 et le nombre des substitutions de classe 69 et 68. En résumé, la valeur $N = 70$ doit être écartée.

$N = 78.$

$\mathcal{G}$ est égal à $2 \times 11 \times 78$ ou $2 \times 7 \times 78$.

Si $\mathcal{G}$ est égal à $2 \times 11 \times 78$, on voit, d'après Sylow, que G renfermerait soixante-six groupes d'ordre 13, ce qui est impossible, comme on le voit en additionnant le nombre des substitutions de classe 77 et 76 et retranchant de $\mathcal{G}$.

Si $\mathcal{G}$ est égal à $2 \times 7 \times 78$, G renferme quatorze groupes d'ordre 13 et un groupe d'ordre 13 est permutable aux substitutions d'un groupe d'ordre 78 qui le contient. Si ce groupe d'ordre 78 était permutable aux substitutions de G, le groupe d'ordre 13 contenu dedans le serait aussi et G ne serait pas primitif. On voit alors facilement que G est

isomorphe à un groupe deux fois transitif de degré 14 et d'ordre $14 \times 13 \times 6$ renfermant une substitution d'ordre 6. G renfermerait une substitution d'ordre 6, par suite, une substitution de classe 78 ne faisant pas partie du groupe alterné de 78 éléments, et ne serait pas primitif.

En résumé, la valeur de N égale à 78 doit être écartée ([1]).

Nous avons ainsi écarté toutes les valeurs de $N \leqq 95$, sauf la valeur $N = 10$. Nous avons vu d'ailleurs que pour $N = 10$ on a un groupe une fois transitif, primitif de classe 8, de degré 10, d'ordre $10 \times 3 \times 2$.

Remarque. — Un groupe de classe $N - 2$ et de degré N ne contient que $\frac{\mathcal{G}}{2\mathcal{K}}$ groupes d'ordre $\mathcal{K}$ laissant chacun deux lettres immobiles. Si K laisse α et β immobile, il y a alors, dans G, $\mathcal{K}$ substitutions de la forme

$$V = (\alpha\beta)\ldots.$$

Donc :

Théorème. — *Soit dans un groupe* G *de classe* $N - 2$ *et de degré* N *transitif,* K *le groupe d'ordre* $\mathcal{K}$ *qui laisse les lettres* α *et* β *immobiles : il y a, dans* G, $\mathcal{K}$ *substitutions de la forme*

$$V = (\alpha\beta)\ldots$$

et G *doit être d'ordre pair.*

Ce théorème aurait pu nous servir à écarter le groupe de degré 77 et d'ordre $3 \times 19 \times 77$ une seule fois transitif.

TROISIÈME PARTIE.

DES GROUPES TRANSITIFS DE CLASSE N — 3 ET DE DEGRÉ N.

Parmi eux nous ne considérerons que les groupes primitifs.

Soit G un groupe primitif de classe $N - 3$ et de degré N; H_α le

---

([1]) Les groupes de degré 96 et 100 s'écartent par des procédés analogues.

groupe de G qui laisse la lettre α immobile. H_α renferme toujours un groupe $H_{\alpha\beta\beta'}$ laissant deux lettres β, β', autres que α, immobiles. On a évidemment

$$N = n\mathfrak{h}_{\alpha\beta\beta'} + 3,$$

$\mathfrak{h}_{\alpha\beta\beta'}$ étant l'ordre de $H_{\alpha\beta\beta'}$.

Nous distinguerons différents cas :

1° Il existe dans H_α un groupe $H_{\alpha\beta} > H_{\alpha\beta\beta'}$ laissant immobile une des deux lettres β, β' seulement, avec la lettre α.

Supposons que $\beta', \gamma_1, \ldots, \gamma_{\sigma-1}$ soient les lettres que $H_{\alpha\beta}$ substitue à β' et que, par suite, il permute exclusivement entre elles et soient

$$S_1, \quad S_2, \quad \ldots, \quad S_{\mathfrak{h}_{\alpha\beta\beta'}}$$

les substitutions de $H_{\alpha\beta\beta'}$,

$$T = (\beta'\gamma_i\ldots)\ldots$$

une substitution de $H_{\alpha\beta}$. Il y a évidemment, dans $H_{\alpha\beta}$, σ substitutions $S_j T$ qui sont de la forme $(\beta'\gamma_i\ldots)\ldots$ et pas d'autres. On voit ainsi que

$$\mathfrak{h}_{\alpha\beta} = \sigma\mathfrak{h}_{\alpha\beta\beta'} = \mathfrak{h}_{\alpha\beta\beta'}(n'\mathfrak{h}_{\alpha\beta\beta'} + 1).$$

On voit encore, comme au début de la deuxième partie de ce Chapitre, qu'aucune des substitutions de $\mathfrak{h}_{\alpha\beta}$ autre que l'unité ne peut laisser immobile une lettre δ différente des lettres α, β, β', $\gamma_1, \ldots, \gamma_{\sigma-1}$. $H_{\alpha\beta}$ permute donc transitivement $\mathfrak{h}_{\alpha\beta}$ à $\mathfrak{h}_{\alpha\beta}$ les lettres différentes de ces $\sigma + 2$ lettres, et

$$N - 2 = \sigma + k\mathfrak{h}_{\alpha\beta}.$$

Ceci posé, si H_α contient une substitution remplaçant β par β', il permute transitivement entre elles $1 + \sigma + k'\mathfrak{h}_{\alpha\beta}$ lettres. D'une substitution remplaçant β par δ on déduit $\mathfrak{h}_{\alpha\beta}$ substitutions remplaçant β par δ et pas plus, en sorte que

$$\mathfrak{h}_\alpha = (1 + \sigma + k'\mathfrak{h}_{\alpha\beta})\mathfrak{h}_{\alpha\beta} = \sigma'\mathfrak{h}_{\alpha\beta}.$$

Si H_α ne contient aucune substitution remplaçant β par β', il per-

mute transitivement entre elles $1+k''\mathfrak{h}_{\alpha\beta}$ lettres et

$$\mathfrak{h}_\alpha = (1+k''\mathfrak{h}_{\alpha\beta})\,\mathfrak{h}_{\alpha\beta} = \sigma''\mathfrak{h}_{\alpha\beta}.$$

2° Le groupe $H_{\alpha\beta}$ se confond avec le groupe $H_{\alpha\beta\beta'}$. Si $H_{\alpha\beta'}$ ne se confondait pas avec $H_{\alpha\beta\beta'}$, on appliquerait les mêmes raisonnements que tout à l'heure. Nous supposerons donc $H_{\alpha\beta} = H_{\alpha\beta'} = H_{\alpha\beta\beta'}$, c'est-à-dire que toute substitution de H_α, laissant β ou β' immobile, laisse forcément β et β' immobiles simultanément. On a évidemment

$$N - 3 = n\,\mathfrak{h}_{\alpha\beta\beta'}.$$

Ceci posé, si H_α contient une substitution remplaçant β par β', elle doit être de la forme $(\beta\beta')\ldots$, d'après ce qu'on vient de dire. Si elle déplace toutes les lettres sauf α, $N-3$ doit être pair, chacun de ses cycles devant renfermer un nombre pair de lettres; si elle laisse deux lettres autres que α immobiles, elle sera régulière et $N-3$ sera pair; enfin, si elle ne laisse immobile qu'une lettre autre que α, elle sera encore régulière et d'ordre 2, mais $N-2$ sera pair. En tout cas, H_α substituera $2p$ lettres à β, et

$$\mathfrak{h}_\alpha = 2p\,\mathfrak{h}_{\alpha\beta\beta'}$$

avec

$$2p = 2 + p_1\mathfrak{h}_{\alpha\beta\beta'}.$$

Si, au contraire, H_α ne contient aucune substitution $(\beta\beta')\ldots$, H_α substitue, à β, $(1+p'\mathfrak{h}_{\alpha\beta\beta'})$ lettres, et forcément autant à β', parce que

$$\mathfrak{h}_\alpha = \mathfrak{h}_{\alpha\beta\beta'}(1+p'\mathfrak{h}_{\alpha\beta\beta'}).$$

Nous nous contenterons, pour ces groupes, d'établir quelques propriétés.

Si l'on applique à ces groupes le théorème général de la page 51, on voit, en particulier, la propriété suivante :

Théorème. — *Étant donné un groupe* G *transitif de degré* N *et d'ordre* $\mathfrak{g} = \mathfrak{h}N$, H *étant le groupe de* G *qui laisse une lettre immobile, tout groupe* G′ *d'ordre* $\mathfrak{g}' \equiv 0 \pmod{N}$ *contenu dans* G *est transitif si* N *n'est divisible ni par* 2, *ni par* 3.

Nous allons encore voir quels sont ceux de ces groupes G qui sont de classe r^2, r étant un nombre premier > 2 et G primitif.

Pour ces groupes, $\mathfrak{H}_{\alpha\beta\beta'}$ peut être égal à r ou à r^2 :

1° $\mathfrak{H}_{\alpha\beta\beta'} = r^2$. — $H_{\alpha\beta\beta'}$ est transitif entre r^2 lettres : si $H_{\alpha\beta}$ est différent de $H_{\alpha\beta\beta'}$, il sera 2 fois transitif; si G est primitif, H_α déplaçant toutes les lettres sera 3 fois transitif, et G 4 fois transitif, ce qui ne peut avoir lieu, puisque le seul groupe 4 fois transitif de classe N — 3 et de degré N est un groupe trouvé par M. Mathieu et de classe 8 [Jordan, *Recherches sur les substitutions* (*Journal de Liouville*; 1872)].

Si $H_{\alpha\beta} = H_{\alpha\beta\beta'} = H_{\alpha\beta'}$, H_α devant déplacer toutes les lettres serait d'ordre $r^2(r^2+2)$ et transitif, ce qui est absurde, parce que r^2+2 n'est pas pair, ou serait d'ordre $2r^2$, et contiendrait une substitution d'ordre pair $(\beta\beta')\ldots$ dont tous les cycles, sauf le cycle $(\beta\beta')$, déplacent le même nombre pair de lettres. En élevant cette substitution, qui déplace r^2+1 lettres à une puissance impaire convenable, on en déduira, puisque G est de classe r^2, une substitution d'ordre 2 à $\frac{r^2+1}{2} = 2h+1$ cycles, ne faisant pas partie du groupe alterné. G contiendrait alors un groupe G' d'ordre $\mathcal{G}' = r^2(r^2+3) = \frac{\mathcal{G}}{2}$ permutable à ses substitutions, qui admet une répartition de ses lettres 3 à 3, en sorte que r^2+3 est $\equiv 0 \pmod 3$ et $r = 3$, $\mathcal{G} = 9 \times 2 \times 12$.

On sait d'ailleurs, d'après M. Jordan (*Comptes rendus*, 2 octobre 1871), qu'il n'existe aucun groupe primitif de classe 9. Le cas où $\mathfrak{H}_{\alpha\beta\beta'} = r^2$ avec r premier > 2 doit donc être écarté.

2° $\mathfrak{H}_{\alpha\beta\beta'} = r$. — Nous allons examiner successivement les quatre cas distingués plus haut.

Dans les deux premiers cas

$$\mathfrak{H}_{\alpha\beta} = r(1+n'r) \qquad \text{avec} \qquad n' > 0,$$

le nombre des lettres de G est

$$N = r^2+3 = 2+(1+n'r)+kr(1+n'r),$$

d'où

$$r^2+1 = (1+n'r)(1+kr),$$

ce qui ne peut avoir lieu que si $k = 0$ et $n' = r$. $H_{\alpha\beta}$ est donc transitif entre $r^2 + 1$ lettres et H_α est 2 fois transitif entre $r^2 + 2$ lettres, parce que, G étant primitif, H_α doit déplacer toutes les lettres. H_α serait donc 2 fois transitif, de classe r^2 et de degré $r^2 + 2$, ce que nous savons impossible si $r > 2$.

Dans le troisième cas, on a une substitution de la forme $(\beta\beta')\ldots$ qui est d'ordre pair, dont tous les cycles déplacent un nombre pair de lettres, et qui déplace $r^2 + 1$ lettres. On en déduit évidemment une substitution d'ordre 2 non contenue dans le groupe alterné et l'on voit encore que $r = 3$. Dans ce cas, $\mathcal{G}$ serait égal à $3 \times 2 \times 12$ et l'on sait, d'après M. Jordan, que G ne peut être primitif.

Dans le quatrième cas, p' serait égal à 0, $\mathcal{G} = r(r^2 + 3)$ et G ne serait pas primitif.

Enfin le cas où $r = 2$ doit également être écarté, d'après M. Jordan (*Comptes rendus*, 2 octobre 1871).

En résumé, *il n'existe aucun groupe primitif de classe* $N - 3$ *et de degré* N, *pour lequel* $N - 3 = r$, r^2 *étant premier.*

Propriétés des groupes de classe $N - i$ et de degré N, au moins $i - 1$ fois transitifs ($i \geqq 3$).

Des procédés analogues à ceux employés pour les groupes de classe $N - 2$ et de degré N permettent d'établir la propriété suivante :

Pour les 77 *premières classes, il n'existe d'autre groupe* 3 *ou* 4 *fois transitif de classe* $N - 3$ *et de degré qu'un groupe de classe* 8 *et de degré* 11, 4 *fois transitif* (groupe cité par M. Jordan dans son énumération des groupes primitifs pour les 17 premiers degrés).

On en conclut facilement :

Pour les 100 *premières classes, il n'y a qu'un groupe de classe* 8 *et de degré* 12, 5 *fois transitif qui appartienne aux groupes de classe* $N - 4$ *et de degré* N *au moins* 4 *fois transitif* (groupe cité également par M. Jordan).

Pour les 100 *premières classes, il n'existe aucun groupe de classe* $N - i$ *et de degré* N, *au moins i fois transitif, i étant* > 4.

Enfin, en appliquant aux groupes deux fois transitifs de classe N — 3 et de degré N les propriétés établies au théorème III de la deuxième partie de ce Chapitre, on arrive encore à la propriété suivante :

Pour les 100 *premières classes, il n'existe aucun groupe* 2 *fois et* 2 *fois seulement transitif de classe* N — 3 *impaire et de degré* N.

D'où l'on conclut :

Pour les 100 *premières classes, il n'existe aucun groupe* $i-1$ *fois et* $i-1$ *fois seulement transitif de classe* $N-i$ *impaire et de degré* N ($i \geqq 3$).

Enfin, d'une propriété établie à la page 77, on conclut :

Il n'existe : 1° *aucun groupe de classe* $p^{2\alpha}$ *et de degré* $p^{2\alpha}+i$ *au moins* $i-1$ *fois transitif;* 2° *aucun groupe de classe* $p^{2\alpha+1}$ *et de degré* $p^{2\alpha+1}+i$ *au moins* $i-1$ *fois transitif avec* $p = 4h+1$; *p étant dans les deux cas un nombre premier impair* ($i \geqq 2$),

et plus généralement :

Il n'existe aucun groupe de classe $4h+1$ *et de degré* $4h+i+1$ *qui soit au moins* $i-1$ *fois transitif* ($i \geqq 2$).

CHAPITRE III.

SUR UNE GÉNÉRALISATION DE LA FORMULE DE SYLOW.

Nous avons déjà rappelé que M. Sylow a montré que, étant donné un groupe G d'ordre $\mathcal{G}$, si p^m est la plus haute puissance d'un nombre premier p qui divise $\mathcal{G}$, G contient un groupe H d'ordre p^m et

$$\mathcal{G} = p^m \nu (np + 1),$$

$p^m\nu$ étant l'ordre du groupe des substitutions de G permutables à H. Il a également montré que tous les groupes de G d'ordre p^m sont les transformés de H par les substitutions de G et en nombre $np+1$ (*Mathematische Annalen*, t. V).

Nous allons donner une nouvelle démonstration de cette formule et en même temps la généraliser.

Des groupes échangeables et des suites associées.

M. Serret (p. 283 du t. II du *Cours d'Algèbre supérieure*) a défini deux groupes échangeables, deux groupes tels que, étant donnée une substitution u et t de chacun d'eux U et T, on ait toujours

$$ut = t'u',$$

t' étant une substitution de T, u' une substitution de U.

Il a démontré (p. 292) que, si U et T n'ont aucune substitution commune, le groupe (U, T) dérivé de U et de T était d'ordre $\upsilon\varpi$ et avait toutes ses substitutions de la forme ut ou $t'u'$ indifféremment. Il est facile de voir de même que, si U et T ont des substitutions communes, et si H est le plus grand groupe commun, (U, T) jouit des mêmes propriétés et est d'ordre

$$\frac{\upsilon \times \varpi}{\mathfrak{h}}.$$

Soient alors $1, h_2, \ldots, h_{\mathfrak{H}}$ les substitutions de H,

$$(1) \quad \left\{ \begin{array}{llll} 1, & h_2, & \ldots, & h_{\mathfrak{H}}, \\ t_2^{(\alpha)}, & t_2^{(\alpha)} h_2, & \ldots, & t_2^{(\alpha)} h_{\mathfrak{H}}, \\ \ldots, & \ldots\ldots, & \ldots, & \ldots\ldots \end{array} \right.$$

ou

$$(2) \quad \left\{ \begin{array}{llll} 1, & h_2, & \ldots, & h_{\mathfrak{H}}, \\ t_2^{(\beta)}, & h_2 t_2^{(\beta)}, & \ldots, & h_{\mathfrak{H}} t_2^{(\beta)}, \\ \ldots, & \ldots\ldots, & \ldots, & \ldots\ldots, \end{array} \right.$$

les substitutions de T. Si l'on caractérise chacune des lignes d'un de ces tableaux par une de ses substitutions choisie arbitrairement, $t_i^{(\alpha)}$ ou $t_j^{(\beta)}$, par exemple, nous dirons que $t_i^{(\alpha)}$ ou $t_j^{(\beta)}$ est *le représentant par rapport à* H ou simplement *le représentant* de la ligne $t_i^{(\alpha)}, h_2 t_i^{(\alpha)}, \ldots, t_i^{(\alpha)} h_{\mathfrak{H}}$ ou de la ligne $t_i^{(\beta)}, h_2 t_i^{(\beta)}, \ldots, h_{\mathfrak{H}} t_i^{(\beta)}$ respectivement.

Soit alors u une substitution de U; on aura

$$(3) \qquad htu = u'h't',$$

t et t' étant des représentants; par suite,

$$htu = u'h'h_{\alpha'}^{-1}h_{\alpha'}t',$$

et

$$h_{\beta'}htu = h_{\beta'}u'h't'.$$

Réciproquement, si

$$h_{\beta'}tu = u'_1h'_1t'_1,$$

on a

$$u'_1h'_1t'_1 = h_{\beta'}h^{-1}u'h't'$$

et

$$t't_1'^{-1} = u'_2 = h''^{-1}$$

ou

$$t'_1 = h''t',$$

parce que u'_2 est commun à U et T.

On en conclut que, u étant donné, si l'on fait entrer dans une égalité de la forme (3) successivement tous les éléments de la ligne du tableau (2) qui a pour représentant t, toutes les substitutions $h't'$ qui

entrent dans le deuxième membre de l'égalité (3) appartiennent à la ligne du tableau (2) qui a pour représentant t'.

On pourrait montrer une propriété analogue pour les lignes du tableau (1). Mais, sauf indication contraire, nous ne considérerons que le tableau (2), les propriétés établies ayant, en général, leurs analogues pour le tableau (1).

Dès lors nous exprimerons la propriété que nous venons d'établir en disant que la substitution u associe la ligne $h't'$ à la ligne ht, ou le représentant t' au représentant t.

La substitution u^{-1} associe évidemment le représentant t au représentant t' : t' et t seront dits des *représentants associés par les substitutions de* U.

Si l'on considère successivement toutes les substitutions de U, elles associeront à t un certain nombre de représentants t, t', t'', ..., car t est évidemment associé à t par la substitution 1. Alors si

$$tu = u'h't',$$

$$tu_1 = u''h''t'',$$

on en tire

$$u''h''t''u_1^{-1}u = u'h't',$$

$$h''t''(u_1^{-1}u) = (u''^{-1}u')h't',$$

c'est-à-dire que t' et t'' sont associés par les substitutions de U. Donc :

Deux représentants associés à un même troisième par U *sont associés entre eux par* U.

La suite des représentants t, t', t'', ... qui sont associés entre eux par U sera dite *une suite de représentants associés par* U, ou, plus simplement, *une suite associée*.

Les $\frac{\mathfrak{G}}{\mathfrak{H}}$ représentants de T pourront ainsi être répartis en un certain nombre de suites associées. La condition nécessaire et suffisante pour qu'une suite associée ne compte qu'un seul représentant est que U soit permutable à ce représentant. La première ligne du tableau (2) considéré, qui admet comme représentant la substitution 1, est toujours dans ce cas. On en conclut que T comprendra toujours au moins deux suite associées.

Propriétés des suites associées.

Soit un certain nombre de suites de représentants associés de T par U

$$(4)\qquad \begin{cases} t_1^{(0)}, & t_2^{(0)}, & \ldots, \\ t_1^{(1)}, & t_2^{(1)}, & \ldots, \\ t_1^{(2)}, & t_2^{(2)}, & \ldots, \\ \ldots, & \ldots, & \ldots, \end{cases}$$

chaque ligne formant une suite.

Si

$$t_i^{(i')} u = u_1 t_{i_1}^{(i')},$$
$$t_j^{(j')} u_1 = u_2 t_{j_1}^{(j')},$$
$$t_k^{(k')} u_2 = u_3 t_{k_1}^{(k')},$$

par exemple, on en tire

$$(5)\qquad t_k^{(k')} t_j^{(j')} t_i^{(i')} u = u_3 t_{k_1}^{(k')} t_{j_1}^{(j')} t_{i_1}^{(i')},$$

ce qui montre que les représentants associés avec un produit $t^{(k')} t^{(j')} t^{(i')}$ d'un certain nombre de représentants du tableau (4) peuvent être mis sous la même forme, c'est-à-dire sous la forme d'un produit d'un même nombre de représentants tels que ceux qui occupent la même place dans chacun des produits sont associés entre eux, ou appartiennent à une même ligne de (4).

Si, en particulier, $k' = j' = i'$, c'est-à-dire si les représentants considérés appartiennent à une même suite, et si l'on forme le groupe T′ dérivé des représentants de cette suite et de H, on voit que les divers représentants qui font partie de T′ sont associés exclusivement entre eux et que T′ est échangeable à U. Donc :

Théorème. — *Étant donnés deux groupes échangeables,* T *et* U, *et soit* H *le groupe des substitutions qui leur sont communes : on n'obtiendra que des groupes de* T *contenant* H *et échangeables à* U, *en considérant les groupes dérivés de* H *et de chacune des suites*

associées de T *par* H. *On obtiendra ainsi, en particulier, tous les groupes minima de* T *échangeables à* U.

Remarque. — En formant le groupe dérivé de H et de plusieurs suites associées de T par U, on n'obtiendra également que des groupes de T contenant H et échangeables à U.

Groupe correspondant à chaque suite associée.

Soit u une substitution quelconque de U, t, t', ..., $t^{(q-1)}$ les q représentants d'une suite associée : u associera, par exemple, t' à t, t'' à t', ...; $t^{(i+1)}$ à $t^{(i)}$, $t^{(i+2)}$ à $t^{(i+1)}$, ..., au moyen de l'égalité (3). A u on pourra donc faire correspondre la substitution $\begin{pmatrix} t\ t' \ldots t^{(i)} & t^{(i+1)} \ldots \\ t'\ t'' \ldots t^{(i+1)} & t^{(i+2)} \ldots \end{pmatrix}$ entre les q lettres t, t', ..., $t^{(q-1)}$. A chaque substitution de U correspondra alors une substitution analogue; si, d'ailleurs,

$$\begin{aligned} tu &= u'h't', \\ t'u_1 &= u'_1 h'_1 t^{(j)}, \\ t(uu_1) &= u'h'u'_1 h'_1 t^{(i)} = u''h''t^{(j)}, \end{aligned}$$

en sorte que si à u correspond la substitution $\theta = (tt'\ldots)\ldots$ entre les q lettres t considérées, si à u_1 correspond la substitution $\theta_1 = (t' t^{(j)}\ldots)\ldots$ entre les mêmes lettres t, à uu_1 correspondra la substitution $\theta\theta_1$ entre ces lettres t. Les substitutions θ, θ_1, ... forment d'ailleurs un groupe Θ. D'après ce qu'on vient de voir, Θ sera isomorphe à U. Donc :

A chaque suite associée Q *de* T *par* U, t, t', ..., $t^{(q-1)}$, *on peut faire correspondre un groupe de substitutions* Θ *entre les* q *lettres* t, t', ..., $t^{(q-1)}$ *isomorphe à* U. *Ce groupe est évidemment transitif et, par suite,* q *est un diviseur de* $\mathfrak{v}$.

Soit $\mathfrak{S}$ l'ordre de ce groupe ; si $\mathfrak{L}$ est l'ordre du groupe L de U correspondant à la substitution 1 de Θ et dont les substitutions u sont telles que

$$t^{(i)} u t^{(i)-1} = u'h',$$

$t^{(i)}$ prenant toutes les q valeurs $t, t', \ldots, t^{(q-1)}$. Si, d'ailleurs, $\frac{\mathfrak{M}}{\mathfrak{L}}$ est le nombre des substitutions de Θ, laissant t immobile, il y a dans $U\mathfrak{M}$ substitutions pour lesquelles

$$tu_1 t^{-1} = u'_1 h'_1,$$

t étant donné. Ces $\mathfrak{M}$ substitutions forment un groupe M qui est le plus général jouissant de cette propriété, et qui contient évidemment L. L'égalité

$$h'^{-1}_2 u'^{-1}_2 tu_2 = t'$$

montre d'ailleurs que les q groupes M correspondant à $t, t', \ldots, t^{(q-1)}$ sont les transformés d'un d'entre eux par les substitutions de U. Dès lors L est le plus grand groupe de M qui soit permutable aux substitutions de U.

L'égalité $q\mathfrak{M} = \mathfrak{v}$ montre le théorème suivant :

Théorème. — *A une suite associée de* q *représentants de* T *par* U *correspondent dans* U *un certain nombre de groupes d'ordre* $\frac{\mathfrak{v}}{q}$, *qui sont les transformés les uns des autres par les substitutions de* U; *chacun de ces groupes d'ordre* $\frac{\mathfrak{v}}{q}$ *est toujours transformé par un au moins des représentants en un groupe de* U.

Remarque. — Un groupe H quelconque contenu dans un groupe T lui est toujours échangeable. On peut donc toujours lui appliquer ce qui précède.

Théorème. — U *et* T *étant deux groupes échangeables et* H *le groupe des substitutions communes,* H′ *le groupe des substitutions de* T *permutables à* U, *soit* N_q *le nombre des suites associées de* q *représentants :* $q\,N_q$ *est divisible par* $\frac{\mathfrak{H}'}{\mathfrak{H}} = N_1$.

En effet, soient $1, h_2, \ldots, h_\beta$ les substitutions de H,

$$(6)\quad \begin{cases} 1, & h_2, & \ldots & h_\beta, \\ t_2, & h_2 t_2, & \ldots, & h_\beta t_2, \\ \ldots, & \ldots\ldots, & \ldots, & \ldots\ldots, \\ t_{N_1}, & h_2 t_{N_1}, & \ldots, & h_\beta t_{N_1} \end{cases}$$

les substitutions de H′,

$$(7)\quad \begin{cases} 1,\ h_2, \ \ldots, h_\beta; & t_2, \ \ldots, h_\beta t_2; & \ldots; & t_{N_1} \ , \ldots, h_\beta t_{N_1}; \\ \tau_2, h_2\tau_2, \ldots, h_\beta \tau_2; & t_2\tau_2, \ldots, h_\beta t_2 \tau_2; & \ldots; & t_{N_1}\tau_2, \ldots, h_\beta t_{N_1}\tau_2; \\ \ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots & \ldots & \ldots\ldots\ldots\ldots \end{cases}$$

les substitutions de T.

Soient $\theta, \theta' \ldots, \theta^{(q-1)}$ les q représentants d'une suite associée de T par U et $q > 1$. On a toujours

$$\theta u = u'\theta'.$$

Si t_i est un des représentants $t_2, \ldots, t_{N_1}$, la suite

$$t_i\theta, \quad t_i\theta', \quad \ldots, \quad t_i\theta^{(q-1)}$$

est une suite associée de q représentants.

En effet, d'abord ces représentants sont différents, car

$$t_i\theta = ht_i\theta^{(j)}$$

entraîne

$$\theta = h'\theta^{(j)},$$

parce qu'évidemment H est permutable aux substitutions de H′. On est donc conduit à un résultat contraire à l'hypothèse.

De plus, ces q représentants sont associés, car

$$t_i\theta u = t_i u'\theta' = u'_1 t_i\theta'.$$

Enfin, toute substitution associée à $t_i\theta$, par exemple, admet un de ces représentants, puisque

$$t_i\theta u_1 = u' t'$$

entraîne

$$u' t' = t_i u'_1 \theta^{(j)} = u''_1 t_i \theta^{(j)}$$

et

$$t' = u'^{-1} u''_1 t_i \theta^{(j)};$$

$u'^{-1} u''_1$ fait évidemment partie de T et de U, ou de H,

$$u'^{-1} u''_1 = h_1,$$
$$t' = h_1 t_i \theta^{(j)}.$$

Ceci posé, considérons les N_1 suites associées

$$(8)\qquad \left\{\begin{array}{llll} \theta, & \theta', & \ldots, & \theta^{(q-1)}, \\ t_2\theta, & t'_2\theta, & \ldots, & t_2\theta^{(q-1)}, \\ \ldots\ldots & \ldots\ldots & & \ldots\ldots, \\ t_{N_1}\theta, & t_{N_1}\theta', & \ldots, & t_{N_1}\theta^{(q-1)}, \end{array}\right.$$

chaque ligne formant une suite associée.

Deux de ces suites n'auront un représentant commun que si elles coïncident. Supposons qu'une ligne donnée du tableau (7) contienne α des q représentants de la première ligne de (8), c'est-à-dire que la suite $\theta, \theta', \ldots, \theta^{(q-1)}$ contienne les α représentants

$$(9)\qquad \theta, \quad t'\theta, \quad \ldots, \quad t^{(\alpha-1)}\theta$$

et qu'il n'y en a pas $\alpha + 1$. Soit θ_1 un autre des q représentants $\theta, \ldots, \theta^{(q-1)}$; on a

$$(10)\qquad \left\{\begin{array}{l} \theta u = u_1 \theta_1, \\ t'\theta u = t' u_1 \theta_1 = u'_1 t' \theta_1, \\ \ldots\ldots\ldots\ldots, \\ t^{(\alpha-1)}\theta u = t^{(\alpha-1)} u_1 \theta_1 = u_1^{(\alpha-1)} t^{(\alpha-1)} \theta_1. \end{array}\right.$$

La première ligne de (8) contiendra donc les α représentants

$$(11)\qquad \theta_1, \quad t'\theta_1, \quad \ldots, \quad t^{(\alpha-1)}\theta_1.$$

Ces représentants sont différents; si de plus on avait

$$t^{(k)}\theta = h t^{(l)}\theta_1$$

avec k et $l < \alpha$, on déduirait

$$\theta_1 = t^{(l)-1} h^{-1} t^{(k)}\theta = h'' t^{(m)}\theta,$$

contrairement à l'hypothèse : les α représentants (11) sont donc différents des α représentants (9).

En continuant de la sorte, on divise les q représentants $\theta, \theta', \ldots, \theta^{(q-1)}$ en $\frac{q}{\alpha}$ séries de α représentants analogues à la série (9), et l'on voit que les α suites

$$(12) \qquad \left\{ \begin{array}{llll} \theta, & \theta', & \ldots, & \theta^{(q-1)}, \\ t'\theta, & t'\theta', & \ldots, & t'\theta^{(q-1)}, \\ \multicolumn{4}{l}{\ldots\ldots\ldots\ldots\ldots\ldots\ldots,} \\ t^{(\alpha-1)}\theta, & t^{(\alpha-1)}\theta', & \ldots, & t^{(\alpha-1)}\theta^{(q-1)}, \end{array} \right.$$

qui font partie de (8), sont toutes identiques à l'une d'entre elles.

En même temps, puisque (9) peut s'écrire aussi

$$t^{(f)}\theta, \quad t^{(f)}t'\theta, \quad \ldots, \quad t^{(f)}t^{(\alpha-1)}\theta \quad \text{avec} \quad f < \alpha,$$

on voit que les α lignes du tableau (6) qui ont pour représentants 1, t', ..., $t^{(\alpha-1)}$ forment un groupe d'ordre $\alpha\mathfrak{z}$, α divisant N_1.

Soit maintenant t_γ un représentant de H' différent de $1, t', \ldots, t^{(\alpha-1)}$. La ligne

$$(13) \qquad t_\gamma\theta, \quad t_\gamma\theta', \quad \ldots, \quad t_\gamma\theta^{(q-1)}$$

du tableau (8) forme une suite associée. Cette suite comprend

$$(14) \qquad t_\gamma\theta, \quad t_\gamma t'\theta, \quad \ldots, \quad t_\gamma t^{(\alpha-1)}\theta$$

et comme on a

$$t_\gamma t^{(i)} t_\gamma^{-1} = t_{\delta^{(i)}},$$

(14) peut s'écrire

$$(15) \qquad t_\gamma\theta, \quad t_{\delta'}(t_\gamma\theta), \quad \ldots, \quad t_{\delta^{(\alpha-1)}}(t_\gamma\theta).$$

Si un autre des représentants (13) était de la forme $t_\varepsilon(t_\gamma\theta)$, on aurait

$$t_\gamma\theta_1 = t_\varepsilon(t_\gamma\theta),$$

d'où

$$\theta_1 = t_\gamma^{-1} t_\varepsilon t_\gamma \theta = t_\eta \theta,$$

contrairement à l'hypothèse.

Si l'on considère alors $t_\gamma\theta_1$, on verra encore que (13) contient les α représentants de la forme $t_{\delta^{(i)}}(t_\gamma\theta_1)$ différents et différents des précédents, car

$$\theta u = u_1 \theta_1$$

entraîne

$$t^{(i)}\theta u = t^{(i)} u_1 \theta_1 = u'_1 t^{(i)}\theta_1,$$
$$t_\gamma t^{(i)}\theta u = t_\gamma u'_1 t^{(i)}\theta_1 = u''_1 t_\gamma t^{(i)}\theta_1,$$

et, en remarquant que $t_\gamma t^{(i)} = t_{\delta^{(i)}} t_\gamma$,

$$t_{\delta^{(i)}}(t_\gamma\theta) u = u''_1 t_{\delta^{(i)}}(t_\gamma\theta_1).$$

En continuant de la sorte, on divise les q représentants $t_\gamma\theta$, $t_\gamma\theta'$, ..., $t_\gamma\theta^{(q-1)}$ en $\frac{q}{\alpha}$ séries de α représentants analogues à la série (15). α nouvelles lignes de (8) seront identiques.

Finalement, on voit que les lignes du tableau (8) sont identiques, α à α, et que chacune d'elles a α représentants dans $\frac{q}{\alpha}$ lignes de (7). De plus le tableau (8) contient évidemment $N_1 \frac{q}{\alpha}$ représentants différents.

En partant d'une suite associée de q représentants non contenue dans (8), on formera un tableau analogue contenant $N_1 \frac{q}{\alpha'}$ représentants différents; et ainsi de suite.

On aura finalement

$$N_1 \frac{q}{\alpha} + N_1 \frac{q}{\alpha'} + \ldots = N_1\left(\frac{q}{\alpha} + \frac{q}{\alpha'} + \ldots\right) = q N_q,$$

$\frac{q}{\alpha}, \frac{q}{\alpha'}, \ldots$ étant entiers, ce qui démontre la proposition. $\alpha, \alpha', \ldots$ sont des diviseurs communs à q et N_1, et H′ contient des groupes d'ordre $\alpha\mathfrak{H}, \alpha'\mathfrak{H}, \ldots$ contenant le groupe H.

Formule de Sylow généralisée.

Étant donnés deux groupes échangeables T et U, ayant en commun $\mathfrak{H}$ substitutions formant un groupe H, le nombre des substitutions de T dont les représentants font partie d'une suite associée de q représentants est $\mathfrak{H}_q N_q$. En faisant prendre à q toutes les valeurs possibles, on obtiendra toutes les substitutions de T, en sorte qu'on peut écrire

$$(16)\qquad \mathfrak{T} = \mathfrak{H}\left[N_1 + 2N_2 + \ldots + qN_q + \ldots + \left(\frac{\mathfrak{T}}{\mathfrak{H}} - 1\right) N_{\frac{\mathfrak{T}}{\mathfrak{H}}-1}\right]$$

Dans cette formule, $N_1 \geqq 1$ et $N_q = 0$ si q ne divise pas $\mathfrak{V}$ et s'il n'existe pas dans U un groupe d'ordre $\frac{\mathfrak{V}}{q}$. De plus, $qN_q \equiv 0 \pmod{N_1}$, d'après le théorème précédent. $N_1\mathfrak{H}$ est l'ordre du groupe des substitutions de T qui sont permutables à U et la parenthèse est divisible par N_1.

En remarquant qu'un groupe H contenu dans un groupe T lui est toujours échangeable, on obtient ce que nous appelons la *formule de Sylow généralisée*. Si, en effet,

$$\mathfrak{H} = p_1^{\alpha_1} \cdots p_i^{\alpha_i},$$

$p_1, \ldots, p_i$ étant des nombres premiers, la formule (16) s'écrira évidemment

$$(17)\qquad \mathfrak{T} = \mathfrak{H}(N_1 + n_1 p_1 + \ldots + n_i p_i),$$

$\mathfrak{H}N_1$ étant l'ordre du groupe des substitutions de T permutables à H.

Il est évident qu'il existera, dans T, $\frac{N_1 + n_1 p_1 + \ldots + n_l p_l}{N_1}$ groupes transformés de H.

Dans le cas particulier où $\mathfrak{H} = p_1^{\alpha_1}$,

$$(18) \qquad \varepsilon = p_1^{\alpha_1}(N_1 + n_1 p_1),$$

et si N_1 était encore divisible par p_1, on en conclurait évidemment l'existence dans T d'un groupe d'ordre $p^{\alpha'_1}$ avec $\alpha'_1 > \alpha_1$, en sorte que si l'on suppose que $p_1^{\alpha_1}$ est la plus haute puissance de p_1, telle qu'il existe dans T un groupe d'ordre $p_1^{\alpha_1}$, N_1 sera forcément premier à p_1, et $p_1^{\alpha_1}$ sera la plus haute puissance de p_1 qui divise ε. On obtient ainsi la formule et le théorème de Sylow.

Comme vérification de la formule (16) ou (17) dans un cas particulier, nous considérerons un groupe 2 fois transitif T et le groupe H qui y laisse une lettre α immobile. Si N est le degré de T, H est maximum dans T et $N_1 = 1$. De plus, le groupe M, le plus général de H, qu'une substitution $t = (\beta\alpha \ldots) \ldots$ de T, ne faisant pas partie de H, transforme en un groupe de H, est évidemment le groupe de H d'ordre $\frac{\mathfrak{H}}{N-1}$ qui laisse β immobile. La formule (16) ou (17) est donc

$$\varepsilon = \mathfrak{H}[1 + (N-1)],$$

et les N représentants de T par rapport à H forment, d'une part, une suite associée de 1 représentant correspondant aux substitutions de H, d'autre part, une suite associée de N — 1 représentants correspondant à toutes les autres substitutions de T.

Applications.

I. — Théorème de Wilson.

La formule de Sylow donne une démonstration du théorème de Wilson, car si l'on considère le groupe formé des $p!$ substitutions entre p lettres, p étant premier,

$$p! = 1.2 \ldots p = p.N_1(1 + np).$$

On sait, d'ailleurs, que $N_1 = p - 1$; donc

$$1.2\ldots(p-2) = (p-2)! = 1 + np \equiv 1 \pmod{p}$$

ou

$$1.2\ldots(p-1) = (p-1)! \equiv -1 \pmod{p}.$$

II. — Théorème de Fermat.

Il peut aussi se déduire de la formule de Sylow, en appliquant un théorème énoncé par M. Serret (p. 304 du t. II du *Cours d'Algèbre supérieure*).

Soit, en effet, p un nombre premier et α un nombre quelconque premier à p. Considérons le groupe G dérivé des substitutions

$$\begin{gathered}(a_1 a_2 \ldots a_\alpha),\\ (b_1 b_2 \ldots b_\alpha),\\ \ldots\ldots\ldots\ldots,\\ (k_1 k_2 \ldots k_\alpha),\\ (a_1 b_1 \ldots k_1)(a_2 b_2 \ldots k_2)\ldots(a_\alpha b_\alpha \ldots k_\alpha) = S,\end{gathered}$$

les lettres étant en nombre αp et la dernière substitution étant d'ordre p. L'ordre $\mathcal{G}$ de ce groupe est

$$\mathcal{G} = p\alpha^p = pN_1(1 + np).$$

Les seules substitutions de G qui transforment S en une de ses puissances sont, d'ailleurs, les substitutions dérivées de S et de la substitution

$$(a_1 a_2 \ldots a_\alpha)(b_1 b_2 \ldots b_\alpha)\ldots(k_1 k_2 \ldots k_\alpha),$$

en sorte que

$$N_1 = \alpha.$$

Donc

$$1 + np = \alpha^{p-1}$$

ou

$$\alpha^{p-1} \equiv 1 \pmod{p} \qquad \text{C. Q. F. D.}$$

III. — Généralisation du théorème précédent.

On obtient une généralisation du théorème précédent en s'appuyant, d'une part, sur le théorème précité (*Algèbre supérieure* de M. Serret), d'autre part, sur la formule (16).

En effet, soit le groupe K dérivé des substitutions

$$A_1 = (a_1\, b_1 \ldots k_1),$$
$$A_2 = (a_2\, b_2 \ldots k_2),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$A_m = (a_m\, b_m \ldots k_m),$$

d'ordre a, et le groupe H formé des puissances de la substitution

$$h = (a_1\, a_2 \ldots a_m)(b_1\, b_2 \ldots b_m)(k_1\, k_2 \ldots k_m).$$

Le groupe T dérivé de H et de K est d'ordre

$$\varpi = m a^m.$$

Les groupes K et H n'ayant aucune substitution commune, on pourra prendre pour représentants de T par rapport à H les diverses substitutions de K.

Ceci posé, considérons les suites associées de q représentants. Elles renferment $q\mathrm{N}_q$ représentants et

$$q\mathrm{N}_q \equiv (\mathrm{mod}\, \mathrm{N}_1), \qquad q\mathrm{N}_q \equiv 0 \qquad (\mathrm{mod}\, q).$$

Si $q\mathfrak{M} = m$, le groupe M le plus général de H, qu'un représentant t élevé à la puissance -1 et faisant partie d'une suite associée de q représentants transforme en un groupe de H, est donc formé des puissances de h^q,

$$h^q = (a_1\, a_{q+1}\, a_{2q+1} \ldots) \ldots \left(a_q\, a_{2q} \ldots a_{\frac{m}{q}q}\right)(b_1\, b_{q+1}\, b_{2q+1} \ldots) \ldots$$

Supposons, par exemple, que

$$t = (c_1 a_1 \ldots) \ldots,$$

d'où

$$t^{-1} = (a_1 c_1 \ldots) \ldots.$$

Il est d'abord évident que si t^{-1} est permutable à M, comme il est dérivé de $A_1, A_2, \ldots, A_m$, il transformera h^q en h^q et, par suite, lui sera échangeable. De plus, t^{-1} devra remplacer a_1 par c_1, a_{q+1} par c_{q+1}, a_{2q+1} par $c_{2q+1}, \ldots, a_{\left(\frac{m}{q}-1\right)q+1}$ par $c_{\left(\frac{m}{q}-1\right)q+1}$. De même, si t^{-1} remplace c_1 par d_1, il remplacera c_{q+1} par $d_{q+1}, \ldots$: en sorte que la substitution t^{-1}, et par suite, la substitution t, devra être dérivée des substitutions

$$\begin{gathered} B_1 = A_1 A_{q+1} A_{2q+1} \ldots A_{\left(\frac{m}{q}-1\right)q+1}, \\ B_2 = A_2 A_{q+2} A_{2q+2} \ldots A_{\left(\frac{m}{q}-1\right)q+2}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ B_q = A_q A_{2q} \; A_{3q} \; \ldots A_{\frac{m}{q}q}, \end{gathered}$$

qui forment un groupe L_q d'ordre a^q.

Réciproquement, q étant choisi arbitrairement parmi les diviseurs de m, si l'on forme les substitutions $B_1, B_2, \ldots, B_q$, le groupe L_q qui en dérive sera tel que toutes ses substitutions soient échangeables à h^q.

Le groupe L_q contient alors toutes les suites associées de q représentants; mais il en contient d'autres, puisqu'il contient, par exemple, les substitutions échangeables à h_q^p, p étant un diviseur quelconque de q.

Soient $p, p', p'', \ldots$ les diviseurs premiers de q différents entre eux. Toutes les substitutions de L_q qui ne font pas partie d'une suite associée de q représentants font partie d'un des groupes $L_{\frac{q}{p}}, L_{\frac{q}{p'}}, L_{\frac{q}{p''}}, \ldots$ d'ordres respectifs $a^{\frac{q}{p}}, a^{\frac{q}{p'}}, a^{\frac{q}{p''}}, \ldots$. Donc

$$q N_q \geqq a^q - \sum_{p^{(i)}} a^{\frac{q}{p^{(i)}}}.$$

Mais les groupes $L_{\frac{q}{p}}$, $L_{\frac{q}{p'}}$, $L_{\frac{q}{p''}}$, ... ont respectivement deux à deux les groupes $L_{\frac{q}{pp'}}$, $L_{\frac{q}{p'p''}}$, ..., $L_{\frac{q}{pp''}}$, ... communs, en sorte que nous avons retranché deux fois les substitutions différentes qui font partie de ces groupes. Donc

$$q\,N_q \leqq a^q - \sum_{(I)} a^{\frac{q}{p}} + \sum_{(II)} a^{\frac{q}{pp'}}.$$

Alors les substitutions communes à deux groupes $L_{\frac{q}{p}}$, $L_{\frac{q}{p'}}$, ... ont été ajoutées dans le deuxième membre $(1 - 2 + 1) = 0$ fois, si elles ne sont pas communes à trois de ces groupes.

En retranchant les ordres de $L_{\frac{q}{pp'p''}}$, ..., les substitutions communes à trois des groupes $L_{\frac{q}{p}}$, $L_{\frac{q}{p'}}$, $L_{\frac{q}{p''}}$ sont ajoutées $(1 - C_3^1 + C_3^2 - 1) = 0$ fois dans le deuxième membre et nous n'introduisons aucune substitution commune à moins de trois des groupes $L_{\frac{q}{p}}$, $L_{\frac{q}{p'}}$, ... Donc

$$q\,N_q \geqq a^q - \sum_{(I)} a^{\frac{q}{p}} + \sum_{(II)} a^{\frac{q}{pp'}} - \sum_{(III)} a^{\frac{q}{pp'p''}}.$$

En ajoutant les ordres de $L_{\frac{q}{pp'p''p'''}}$, ..., les substitutions communes à quatre des groupes $L_{\frac{q}{p}}$, $L_{\frac{q}{p'}}$, ... sont ajoutées $(1 - C_4^1 + C_4^2 - C_4^3 + 1) = 0$ fois et nous n'introduisons aucune substitution commune à moins de quatre groupes $L_{\frac{q}{p}}$, $L_{\frac{q}{p'}}$, ... On continuera de la sorte en remarquant que $(1 - C_f^1 + C_f^2 - C_f^3 + \ldots) = (1-1)^f = 0$, et l'on finira par obtenir un deuxième membre où les substitutions de L_q communes à i des groupes $L_{\frac{q}{p}}$, $L_{\frac{q}{p'}}$, ... seront comptées 0 fois, avec $i \geqq 1$. Ce second membre sera donc égal à $q\,N_q$.

On en déduit la congruence

$$(20) \qquad a^q - \sum_{p} a^{\frac{q}{p}} + \ldots \equiv 0 \pmod{q},$$

qui est une généralisation du théorème de Fermat, puisqu'elle se réduit à

$$a^q - a \equiv 0 \qquad (\operatorname{mod} q),$$

quand q est un nombre premier.

q est, d'ailleurs, évidemment en tout cas un diviseur quelconque de m, et il existe toujours des suites associées de q représentants.

Nous allons donner quelques applications simples de cette formule.

Si $q = pp'$, p et p' étant premiers, différents,

$$q\mathrm{N}_q = a^{pp'} - a^p - a^{p'} + a \equiv 0 \qquad (\operatorname{mod} q);$$

p et p' étant, au contraire, égaux, $q = p^2$,

$$q\mathrm{N}_q = a^{p^2} - a^p \equiv 0 \qquad (\operatorname{mod} q).$$

Si $q = pp'p''$, p, p', p'' étant premiers, différents,

$$q\mathrm{N}_q = a^{pp'p''} - a^{pp'} - a^{p'p''} - a^{p''p} + a^p + a^{p'} + a^{p''} - a \equiv 0 \qquad (\operatorname{mod} q);$$

p'' et p étant égaux et différents de p',

$$q\mathrm{N}_q = a^{p^2p'} - a^{p^2} - a^{pp'} + a^p \equiv 0 \qquad (\operatorname{mod} q);$$

p'', p' et p étant égaux,

$$q\mathrm{N}_q = a^{p^3} - a^{p^2} \equiv 0 \qquad (\operatorname{mod} q).$$

En général, si $q = p^m$, p étant premier,

$$q\mathrm{N}_q = a^{p^m} - a^{p^{m-1}} = a^{p^{m-1}}(a^{p^{m-1}(p-1)} - 1) \equiv 0 \qquad (\operatorname{mod} q),$$

et si a est premier à q

$$a^{\varphi(p^m)} - 1 \equiv 0 \qquad (\operatorname{mod} p^m),$$

ce qui est le théorème appelé *théorème de Fermat généralisé*, dans le cas où le module considéré est une puissance de nombre premier.

IV. T et U étant deux groupes échangeables, il pourra se faire que le groupe M de U, que l'inverse d'un représentant de T par rapport à U transforme en un groupe de U, ne puisse être égal qu'à 1 ou à U. Alors, si $M = 1$, $q\mathfrak{M} = \mathfrak{v}$ donne $q = \mathfrak{v}$. Les suites associées ont donc 1 ou $\mathfrak{v}$ représentants et

$$\mathfrak{E} = \mathfrak{H}(N_1 + \mathfrak{v}N_{\mathfrak{v}}),$$

avec

$$\mathfrak{v}N_{\mathfrak{v}} \equiv 0 \qquad (\operatorname{mod} N_1).$$

Si, en particulier, on considère un groupe T transitif de classe $N-1$ et de degré N, et si l'on prend pour U le groupe H_α qui y laisse une lettre α immobile, on voit que c'est le cas et que, de plus, $N_1 = 1$. Donc

$$\mathfrak{E} = \mathfrak{H}_\alpha(1 + N_{\mathfrak{H}_\alpha}\mathfrak{H}_\alpha).$$

Nous retrouvons ainsi le théorème I de la première partie du Chapitre II. On voit, en même temps que les représentants de T qui ne font pas partie de H_α sont associés $\mathfrak{H}_\alpha$ à $\mathfrak{H}_\alpha$. Dès lors, si H_α n'est pas maximum dans T, T contient un groupe T′ dérivé de H_α et d'une suite associée, d'ordre

$$\mathfrak{E}' = \mathfrak{H}_\alpha(1 + N'_{\mathfrak{H}_\alpha}\mathfrak{H}_\alpha) < \mathfrak{E},$$

d'où l'on déduit à nouveau le théorème III de la première partie du Chapitre II.

Si le groupe T n'était pas transitif, mais était de classe $N-1$ et de degré N, on aurait encore

$$\mathfrak{E} = \mathfrak{H}_\alpha(1 + N_{\mathfrak{H}_\alpha}\mathfrak{H}_\alpha).$$

Ceci posé, soit T un groupe de classe $N-2$ et de degré N transitif, H_α le groupe de T qui laisse la lettre α immobile, K le groupe de H_α ou T qui laisse α et β immobiles.

La considération de H_α et des suites associées qui lui correspondent donne

$$\mathfrak{E} = \mathfrak{H}_\alpha[1 + N_j(1 + N_{\mathfrak{K}}\mathfrak{K}) + N_{\mathfrak{H}_\alpha}\mathfrak{H}_\alpha],$$

avec

$$\mathfrak{z}_\alpha = \mathfrak{x}(1 + N_{\mathfrak{x}}\mathfrak{x}),$$

d'après ce qui précède.

La considération de K donne

$$\varpi = \mathfrak{x}(N'_1 + N'_{\mathfrak{x}}\mathfrak{x}) \qquad \text{avec} \qquad N'_{\mathfrak{x}}\mathfrak{x} \equiv 0 \qquad (\text{mod} N'_1).$$

En remarquant que $\mathfrak{x}$ divise $N - 2$, on obtient le théorème I de la deuxième partie du Chapitre II.

Mais on obtient de plus un autre résultat; en effet,

$$\varpi = \mathfrak{x}(p\mathfrak{x} + 1)[(p\mathfrak{x} + 1)(q\mathfrak{x} + 1) + 1]$$

donne $\frac{\varpi}{\mathfrak{x}} \equiv 2 \ (\text{mod}\,\mathfrak{x})$.

Donc

$$N'_1 \equiv 2 \qquad (\text{mod}\,\mathfrak{x}), \qquad \text{d'où} \qquad N'_1 = 2.$$

Il y a donc dans T des substitutions qui ne font pas partie de K et permutables à K : elles seront de la forme

$$V = (\alpha\beta)\ldots.$$

Elles sont, d'ailleurs, évidemment en nombre $\mathfrak{x}$ et $N'_1 = 2$. C'est le théorème énoncé à la fin de la deuxième partie du Chapitre II.

Théorème. — *Si, dans un groupe* T *de classe* $N - 2$ *et de degré* N *transitif, le groupe qui laisse* α *et* β *immobiles est d'ordre* $\mathfrak{x}$, *il y a, dans* T, $\mathfrak{x}$ *substitutions* V *de la forme* $V = (\alpha\beta)\ldots$ *et* T *doit être d'ordre pair.*

Vu et approuvé :
Paris, le 2 mai 1892,
Le Doyen de la Faculté,
G. DARBOUX.

Vu et permis d'imprimer :
Paris, le 2 mai 1892.
Le Vice-Recteur de l'Académie de Paris,
GRÉARD.

SECONDE THÈSE.

PROPOSITIONS DONNÉES PAR LA FACULTÉ.

Équations générales de l'Hydrodynamique et théorie de M. Helmholtz sur les Wirbelbewegungen.

Vu et approuvé :
Paris, le 2 mai 1892,
LE DOYEN,
G. DARBOUX.

Vu et permis d'imprimer :
Paris, le 2 mai 1892.
LE VICE-RECTEUR DE L'ACADÉMIE DE PARIS,
GRÉARD.

18531 PARIS. — IMPRIMERIE GAUTHIER-VILLARS ET FILS, QUAI DES GRANDS-AUGUSTINS, 55.

